Document Title	Product security Risk Table
Document number / Revision	D001020017 / 01
Date	8-Apr-22
Project	SmartMedic Phase II
Project number	SGTC-NPD-001

		Product Security Risk Tab	le approval	
Approvals	Name	Title	Signature	Date
Author	Deepak Sharma	Design Engineering R&D (Software)		
	Pragya Nidhi	Test Engineering		
Approvers	Vikram Puri	Advanced Operations (Mfg & QA)		
	Sreejith Viswam	Advance Quality Engineer		

Document Revision History:

REV#	Revision Date	Author	Description of Revision
00	30-Aug-21	Deepak Sharma	Initial Release DR1-4 Document was reviewed but not approved and archived, thus archiving
01	8-Apr-22	Deepak Sharma	Document updated as per DR5-7 requirements -Security Controls/Mitigations -Security Risk Control Measures -Implementation of Risk Control Measures -Verification of Risk Control Measures (Effectiveness)

Stryker Confidential Page 1 of 27

System & Asset Identification

Medical Device / System:	SmartMedic
Scope:	SmartMedic -001-02-A-00-00
Date:	<08 April 2022>
Conducted by:	< Author Name / Function / Organization> Deepak Sharma / Design Engineering R&D Software
	<author function="" name="" organization=""></author>

ID#	Asset Type (Information/Physical)	Asset	Asset Description
A01	Physical Asset	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Utilizing computer resources and computing power by adversary, allows various general purpose attacks, such as incl. Ransomware deployment, Bitcoin Mining, abuse of peripheral devices such as WebCam, Microphones, etc., .
A02	Information asset	Tablet OS/network details & Tablet Application	Information about internals of the system (Device identification, software versions, supported protocols, etc.)
A03	Physical Assets	Smart medic (Stryker device) System Component	Monitors local bed status information, alerting caregivers visually, audibly or remotely if preset parameters are compromised.
A04	Information asset	Authentication/Authorisation method of all device(s)/app	Information related to authenication/authorisation data (password/pins/MFA/Biometrics)
A05	Physical Assets	Device Maintainence tool (Hardware/Software)	Device Maintainence tool (Hardware/Software) that patchs and updates Smart Medic Device and Application related to Security
A06	Information asset	Electronic Health Records (EHR)/ Device Component status	Smart device components health status information
A07	Information asset	Interface/API Communication	Communication middleware enables communication and data management for distributed applications.
A08	Physical Assets	Wireless Network device (Scope of HDO)	Devices that are used for communication among the Smart Medic project component.
A09	Information asset	Data at Rest	Use strong encryption algorthim to store data on cloud platform (Smartmedic Device)/tablet
A10	Information asset	Data in Transit	Use strong encryption algorthim to data moving on tablet to cloud platform(Smartmedic Device)/tablet
A11	Information asset	Smart medic app (Stryker Admin Web Application)	Smart medic application for nurse/health worker (Stryker Admin Web Application)
A12	Information asset	Smart medic app (Azure Portal Administrator)	Azure Portal Administrator for Smart medic app
A13	Information asset	Azure Cloud DataBase	Azure Cloud DataBase related to Smart Medic app
A14	Information asset	Health vital data	Health vital data Body temperature. Pulse rate. Respiration rate, weight data, position data, etc.
A15	Information asset	Nurse Station Application	Smart medic web application for nurse/health worker running on the Nurse Station

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

D05788-1, Ver 1

Stryker Confidential Page 2 of 27

Vulnerability Identification

Vuln. ID	Vulnerability Description	Applicable (Yes/No)	Rationale (if Vulnerability not applicable)
V01	Devices with default passwords needs to be checked for bruteforce	Yes	n/a
	attacks		
V02	External communications and exposure for communciation channels	Yes	n/a
	from and to application and devices like tablet and smartmedic device.		
V03	The password complexity or location vulnerability. Like weak	Yes	n/a
****	passwords and hardcoded passwords.	••	<u> </u>
V04	Checking authentication modes for possible hacks and bypasses	Yes	n/a
V05 SBOM	Insecure communications in networks (hospital)	Yes	n/a
V06	Lock of Accet location discovers in cognitive energians manual	Yes	ln /a
V07	Lack of Asset location digaram in security operations manual Lack of configuration controls for IT assets in the informaion system	Yes	n/a n/a
V07	plan	ies	li/a
V08	Ineffective patch management of firware, OS and applications	Yes	n/a
V 00	thoughout the information system plan	163	11/4
V09	Lack of plan for periodic Software Vulnerability Management	Yes	n/a
V10	The static connection digaram between devices and applications with	Yes	n/a
	provision for periodic updation as per changes		
V11	Assest counting system for all instances of product implementation	Yes	n/a
			,
Access points			•
V12	Unprotected network port(s) on network devices and connection	Yes	n/a
	points		
V13	Unprotected external USB Port on the tablet/devices.	Yes	n/a
V14	Unencrypted Network segment through out the information flow	Yes	n/a
V15	Controlled Use of Administrative Privileges over the network	Yes	n/a
Data			
V16	Unencrypted data at rest in all possible locations	Yes	n/a
V17	Unencrypted data in transit in all flowchannels	Yes	n/a
V18	Weak Encryption Implementaion in data at rest and in transit tactical	Yes	n/a
*****	and design wise		1 ,
V19	Weak Algorthim implementation with respect cipher key size	Yes	n/a
InSecure Configurations of Resource		\	
V20	InSecure/not recommended Configuration for Mobile Devices,	Yes	n/a
V21	Laptops, Workstations, and Servers InSecure Configuration for Software/OS on Mobile Devices, Laptops,	Yes	ln /a
V21	Workstations, and Servers	res	n/a
V22	Legacy system identification if any	Yes	n/a
V23	Outdated - Software/Hardware	Yes	n/a
V31	Improper/insufficient provisioning of IOT hub	Yes	n/a
V32	Unsecured communication with unauthenticated 3rd party devices	Yes	n/a
*32	onsecured communication with anadinenticated sta party devices	163	II) u
AuthN management			
V24	Error Info containing sensitive data for Failed Authentication	Yes	n/a
	attempts		
V25	Absence of additional security factor along with user identification	Yes	n/a
V26	Having no limit on the login attempts	Yes	n/a
V27	No session expiry after certain time interval	Yes	n/a
Logging/Monitoring			
V28	Insufficient Logging information	Yes	n/a
V29	Insufficient Access permissions for accessing and modifying Log files	Yes	n/a
Keys & Certificates			
V30	Improper security (for ex., Storage & Access) for Key tokens and	Yes	n/a
	Certificates		
A			

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Stryker Confidential Page 3 of 27

Threat Assessment

#	Threat Event	Description	Threat Source	In Scope (Yes/No)	Rationale (if out of scope)
T01	Deliver undirected malware (CAPEC-185)	Thread source delivers malware by providing removable media prepared with malware. Removable media is e.g. left on a parking lot and picked up by hospital staff. USB stick finds its way to the Navigation System. Malware eploits known a known vulnerability and e.g. gains admin priviledges. Undirected attack on computer systems.	TSA-3 - Skript Kiddies	Yes	n/a
T02	Deliver directed malware (CAPEC-185)	Thread source delivers malware on a removable media which was designed to exploit a known vulnerability of the Navigation System. Directed attack on the Navigation System using knowledge about the Navigation System.	TSA-2 Organization	Yes	n/a
T03	Gaining Access ([S]TRID[E])	This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data	TSA-2 Organization	Yes	n/a
T04	Maintaining Access (TTP)	The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.	TSA-2 Organization	Yes	n/a
T05	Clearing Track (TTP)	This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created	TSA-2 Organization	Yes	n/a
T06	Elevation of privilege (STRID[E])	Identify weaknesses of segregation in terms of administrative and user-level privileges	TSA-2 Organization	Yes	n/a
T07	Denial of service (STRI(D)E)	Find ways to exhaust or drown out legitimate requests	TSA-3 - Skript Kiddies	Yes	n/a
T08	Information disclosure (STR(I)DE)	Fuzz application parameters or arguments to impact application error disclosures. Identify open ports with their respective services. Incite confidentiality and integrity in the browser interface. Identify clear text communications. Review usage of HTTP headers and user-agent profile. Pinpoint usages of API endpoints and application backend technologies.	TSA-2 Organization	Yes	n/a
T09	Data Access (STR[I]DE)	Access user and application data e.g. by a malicious application or script	TSA-3 - Skript Kiddies	Yes	n/a
T10	Open network port exploit (TTP)	Penetrate Open and Unsecured Ports	TSA-3 - Skript Kiddies	Yes	n/a
T11	Brute-force Attack (CAPEC-112)	The brute-force attack contained a dictionary of well-known directories and authentication paradigms present in common webservers.	TSA-2 Organization	Yes	n/a
T12	Social Engineering (TTP)	create custom phishing scams, phone-based attacks and ev	TSA-3 - Skript Kiddies	Yes	n/a
T13	Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	All the actions/events should be properly logged and the content needs to be protected by proper access rights.	TSA-2 Organization	Yes	n/a
T14	Unauthorized Alterations (S[T]RIDE)	This involves modifying registry values, deleting/encrypting Confidential info and uninstalling Any secure applications and renaming/deleting all files/folders	TSA-2 Organization	Yes	n/a

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Stryker Confidential Page 4 of 27

Security Risk Assessment

Security Risk Assessmen	ıt.																												
		_		Adverse Impact	<u> </u>	Т.Т	<u> </u>					Pre-Implementation of Sec	curity Controls							Security Controls/Mitigations		à l				entation of Security Controls			
ID# Thr	reat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	itegrity	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Security Risk Control Measu Level	res Implementation of Risk Contro Measures	l Verification of Risk Control Measures (Effectiveness)	id ential tegrity	Attack Vector	Attack Privileges Complexity Required	User Interaction	Scope CVSS v3.0 Ba	Base Overall Scor	ll Risk Security Risk I re Level	esidual Security Risk Acceptability Justification
1 Deliver un	ndirected malware	Unprotected external USB Port	Tablet Resources - web cam.	1) Malicious utilization of computer resources 2) computing	l j	= .	Ž.												Asset should be behind stateful	1. SOM D001020115 - 23. Malware	Penetration Testing Protocol	Conf	Ava						
(CAPEC-1	ndirected malware 185)	Unprotected external USB Port on the tablet/devices.	microphone, OTG devices, Removable USB, Tablet	Malicious utilization of computer resources 2) computing 3) denial of service attacks, 4) ransomware attack s 5) Bitcoin mining, etc	9,500														firewall 2. Anti-virus with updated virus	Detection/Protection 2. SRS D001020024 - 2.17.6The	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001								
			(Bluetooth, Wifi)	s) bicom mining, etc															Audit/System log capturing any abnormal activity identified/repo	Application shall support the use o									
																			the application 4. Use hardened interfaces (n/w)	& 3.SRS D001020024 - 2.23.1 The	3) DSTC001: GSL-STC-003								
T01	v	13 A)1		Low	Low L	ow Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	39	Low	0.20	3.5	LOW secure tunnel communications ch	innel Application shall have logs of table application and firmware (SmartMedic devices).	4) DSTC001 - GSL-STC-004					#N/A	#N/	/A	
																				4. SRS D001020024 -2.17.2The									
																				Application shall provide secure tunnel Communications channel									
2 7 7	h l . l																												
(CAPEC-1	ndirected marware 185)	on the tablet/devices.	Smart medic (Stryker device) System Component	Malicious utilization of computer resources 2) computing denial of service attacks, A) ransomware attack	g power NA														1. Asset should be behind stateful firewall 2. Anti-virus with updated virus	1. SOM D001020115 - 23. Malware Detection/Protection	Document #: D001020037: 1) DSTC001: GSL-STC-001								
т01	v	13 A	03	4) ransomware attack 5) Bitcoin mining, etc	Low	Low L	ow Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	39	Low	0.2	3.5	definitions 3. Audit/System log capturing any		NA					#N/A	#N/	/A	
																			abnormal activity identified/repo the application 4. Use hardened interfaces (n/w)										
3 Deliver un	indirected malware 185)	External communications and exposure for communication	Smart medic (Stryker device)	1) Malicious utilization of computer resources 2) computing	g power NA						-		_						secure tunnel communications ch LOW 1. Asset should be behind stateful	nnel 1. SOM D001020115 - 23. Malware	Penetration Testing Protocol	\rightarrow					_		
(CAPEC-1	185)	exposure for communciation channels from and to application and devices like tablet and	System Component	3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc															firewall 2. Anti-virus with updated virus	Detection/Protection 2,3,4. SRS D001020025	Document #: D001020037: 1) DSTC001: GSL-STC-001								
T01	v	02 smartmedic device. A	13	J Decom many, etc.	Low	Low L	ow Network	Low	Low	Required	Unchanged	2.1	0.5	3.4	5.5	Low	0.2	3.8	definitions 3. Audit/System log capturing any abnormal activity identified/repo		NA					#N/A	#N/	/A	
																			the application 4. Use hardened interfaces (n/w) secure tunnel communications ch										
4 Deliver un (CAPEC-1	ndirected malware 185)	External communications and exposure for communication channels from and to application	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet	Malicious utilization of computer resources 2) computing denial of service attacks,	ng power NA														1. Asset should be behind stateful firewall	1. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037:								
		and devices like tablet and	Application, Network interface	4) ransomware attack 5) Bitcoin mining, etc															Anti-virus with updated virus definitions	2. SRS D001020024 - 2.17.6The	1) DSTC001: GSL-STC-001								
		smartmedic device.	(Bluetooth, Wifi)																 Audit/System log capturing any abnormal activity identified/repo the application 	ted by anti-malware mechanism	2) DSTC001: GSL-STC-002								
T01	v	02 A	01		Low	Low L	ow Network	Low	Low	Required	Unchanged	2.1	0.5	3.4	5.5	Low	0.2	3.8	the application 4. Use hardened interfaces (n/w) secure tunnel communications ch	innel Application shall have logs of table	3) DSTC001: GSL-STC-003					#N/A	#N/	/A	
																				application and firmware (SmartMedic devices).	4) DSTC001 - GSL-STC-004								
																				4. SRS D001020024 - 2.17.2The Application shall provide secure									
5 Deliver ur (CAPEC-1	indirected malware	Legacy system identification if	Smart medic (Stryker device) System Component	Malicious utilization of computer resources 2) computing denial of service attacks,	g power NA	+													LOW 1. Asset should be behind stateful firewall	tunnel Communications channel 1. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037:								
(Carat-1	. "	7	Journal Component	4) ransomware attack 5) Bitcoin mining, etc															2. Anti-virus with updated virus definitions	2,3,4. SRS D001020025	1) DSTC001: GSL-STC-001								
T01	v	" A	13		Low	Low L	ow Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	41	Low	0.2	3.6	 Audit/System log capturing any abnormal activity identified/repo the application 		NA					#N/A	#N/	/A	
											⊥_ l								the application 4. Use hardened interfaces (n/w) secure tunnel communications ch	innel									
6 Deliver un (CAPEC-1	ndirected malware 185)	Legacy system identification if any	Tablet Resources - web cam, microphone, OTG devices,	Malicious utilization of computer resources 2) computing denial of service attacks,	g power NA														1. Asset should be behind stateful firewall	1. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037:								
			Application, Network interface (Bluetooth, Wifi)	3) denial of service attacks, 4) ransomware attack ss 5) Bitcoin mining, etc															Anti-virus with updated virus definitions Audit/System log capturing any	2. SRS D001020024 - 2.17.6The Application shall support the use o	1) DSTC001: GSL-STC-001								
			(ted by anti-malware mechanism	2) DSTC001: GSL-STC-002								
T01	ľ	22 A)1		Low	Low L	ow Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	41	Low	0.2	3.6	 Use hardened interfaces (n/w) secure tunnel communications ch 		3) DSTC001: GSL-STC-003					#N/A	#N/	/A	
																				application and firmware (SmartMedic devices).	4) DSTC001 - GSL-STC-004								
																				4. SRS D001020024 - 2.17.2The Application shall provide secure									
7 Deliver us (CAPEC-1	indirected malware	Ineffective patch management of firware. OS and applications	Device Maintainence tool (Hardware/Software)	Malicious utilization of computer resources 2) computing denial of service attacks,	g power NA														LOW 1. Asset should be behind stateful firewall	tunnel Communications channel Device maintainence tool not implemented/existing in the SM	Penetration Testing Protocol Document #: D001020037:								
	,	firware, OS and applications thoughout the information system plan	(4) ransomware attack 5) Bitcoin mining, etc															2. Anti-virus with updated virus definitions	platform.	1) DSTC001: GSL-STC-028								
701	ľ	08 A	05		Low	Low L	w Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	Audit/System log capturing any abnormal activity identified/repo the application	ted by						#N/A	#N/	/A	
																			the application 4. Use hardened interfaces (n/w) secure tunnel communications ch	innel									
8 Deliver us (CAPEC-1	ndirected malware 185)	Ineffective patch management of firware, OS and applications	Tablet Resources - web cam, microphone, OTG devices,	Malicious utilization of computer resources 2) computing denial of service attacks,	g power NA														1. Asset should be behind stateful firewall	1. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037:								
		thoughout the information system plan	Removable USB, Tablet Application, Network interface (Bluetooth, Wifi)	4) ransomware attack 5) Bitcoin mining, etc															Anti-virus with updated virus definitions Audit/System log capturing any	2. SRS D001020024 - 2.17.6The Application shall support the use o	1) DSTC001: GSL-STC-001								
			(abnormal activity identified/repo the application	ted by anti-malware mechanism	2) DSTC001: GSL-STC-002								
T01	v	08 A	01		Low	Low L	w Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	 Use hardened interfaces (n/w) secure tunnel communications ch 	innel Application shall have logs of table	3) DSTC001: GSL-STC-003 : 4) DSTC001 - GSL-STC-004					#N/A	#N/	/A	
																				application and firmware (SmartMedic devices).	4)231001-022310-004								
																				SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel									
	h	1 % 3									\vdash																		
(CAPEC-1	ndirected malware 185)	Ineffective patch management of firware, OS and applications thoughout the information	System Component	Malicious utilization of computer resources 2) computing denial of service attacks, 4) ransomware attack	g power NA														1. Asset should be behind stateful firewall 2. Anti-virus with updated virus	Detection/Protection	Document #: D001020037:								
T01	v	system plan O8	13	5) Bitcoin mining, etc	Low	Low L	w Local	Low	Low	None	Unchanged	1.8	0.5	34	5.3	Low	0.2	3.8	definitions 3. Audit/System log capturing any	2,3,4. SRS D001020025	1) DSTC001: GSL-STC-001					#N/A	#N/	/A	
																			abnormal activity identified/repo the application 4. Use hardened interfaces (n/w)	- 1	NA								
10 Deliver u	indirected malware	Lack of plan for periodic Software Vulnerability	Device Maintainence tool	Malicious utilization of computer resources 2) computing	ig power NA						-		_						secure tunnel communications ch 1. Asset should be behind stateful	nnel Device maintainence tool not	Penetration Testing Protocol								
(CAPEC-1	185)	Software Vulnerability Management	(Hardware/Software)	denial of service attacks, ansomware attack															firewall 2. Anti-virus with updated virus	implemented/existing in the SM platform.	Document #: D001020037: 1) DSTC001: GSL-STC-028								
T01	v	09 A	05	5) Bitcoin mining, etc	Low	Low L	w Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	3. Audit/System log capturing any abnormal activity identified/repo	ted by	1) 151 (1001: (651/517-028					#N/A	#N/	/A	
																			the application	.									
11 Deliver us	indirected malware 185)	Lack of plan for periodic Software Vulnerability Management	Tablet Resources - web cam,	Malicious utilization of computer resources 2) computing Applied of computer attacks.	g power NA														LOW 1. Asset should be behind stateful firewall	1. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037:								
(,	Management	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interface (Bluetooth, Wifi)	4) ransomware attack es 5) Bitcoin mining, etc															 Anti-virus with updated virus definitions 	2. SRS D001020024 - 2.17.6The	1) DSTC001: GSL-STC-001								
			(Bluetooth, Wifi)																 Audit/System log capturing any abnormal activity identified/repoths application. 	ted by anti-malware mechanism	2) DSTC001: GSL-STC-002								
T01	v	09 A	01		Low	Low L	w Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	the application 4. Use hardened interfaces (n/w) secure tunnel communications ch	nnel Application shall have logs of table	3) DSTC001: GSL-STC-003					#N/A	#N/	/A	
																				application and firmware (SmartMedic devices).	4) DSTC001 - GSL-STC-004								
																				4. SRS D001020024 -2.17.2The Application shall provide secure									
12 Deliver un	indirected malware 185)	Lack of plan for periodic	Smart medic (Stryker device)	Malicious utilization of computer resources 2) computing denial of service attacks,	ng power NA	+		+	1		+					\vdash			LOW 1. Asset should be behind stateful	tunnel Communications channel 1. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037:			+ + -	-				
(CAPEC-1	185]	Software Vulnerability Management	System Component	3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc															firewall 2. Anti-virus with updated virus	2,3,4. SRS D001020025	Document #: D001020037: 1) DSTC001: GSL-STC-001								
T01	v	09 A	03	o, _ncom mmng, e.c	Low	Low L	w Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	definitions 3. Audit/System log capturing any abnormal activity identified/repo the application		NA					#N/A	#N/	/A	
																			the application 4. Use hardened interfaces (n/w) secure tunnel communications ch	li.									
13 Deliver un (CAPEC-1	indirected malware 185)	Unprotected network port(s) on network devices and connection	Tablet Resources - web cam, microphone, OTG devices.	Malicious utilization of computer resources 2) computing 3) denial of service attacks, ansomware attack	ng power NA	+													1. Asset should be behind stateful firewall		Penetration Testing Protocol Document #: D001020037:								
		points	Removable USB, Tablet Application, Network interface (Bluetooth, Wifi)	4) ransomware attack 5) Bitcoin mining, etc															Anti-virus with updated virus definitions	2. SRS D001020024 -2.17.6The	1) DSTC001: GSL-STC-001								
			(Biuetooth, Wifi)																the application	ted by anti-malware mechanism	2) DSTC001: GSL-STC-002								
T01	v	12 A	01		None	None H	gh Network	Low	High	None	Unchanged	12	0.6	3.6	4.9	Low	0.2	3.9	 Use hardened interfaces (n/w) 	innel Application shall have logs of table	3) DSTC001: GSL-STC-003					#N/A	#N/	/A	
																				application and firmware (SmartMedic devices).	4) DSTC001 - GSL-STC-004								
																				4. SRS D001020024 -2.17.2The Application shall provide secure									
14 Deliver un	indirected malware	Unprotected network port(s) on network devices and connection	Smart medic (Stryker device)	Malicious utilization of computer resources 2) computing Assistant accompany attacks.	g power NA	+													LOW 1. Asset should be behind stateful	tunnel Communications channel 1. SOM D001020115 - 23. Malware	Penetration Testing Protocol	+		+ +					
(CAPEC-1	au.0J	network devices and connection points	System Component	3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc															firewall 2. Anti-virus with updated virus definitions	Detection/Protection 2,3,4. SRS D001020025	Document #: D001020037: 1) DSTC001: GSL-STC-001								
T01	v	12 A	03	1	None	None H	gh Network	Low	High	None	Unchanged	12	0.6	3.6	4.9	Low	0.2	3.9	Audit/System log capturing any abnormal activity identified/repo		NA NA					#N/A	#N/	/A	
																			the application 4. Use hardened interfaces (n/w)	&									
15 Deliver un (CAPEC-1	indirected malware 185)	Unencrypted data at rest in all possible locations	Tablet Resources - web cam, microphone, OTG devices.	Malicious utilization of computer resources 2) computing denial of service attacks,	ig power NA	+													secure tunnel communications ch 1.0W 1. Asset should be behind stateful firewall	1. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037:								
			microphone, OTG devices, Removable USB, Tablet Application, Network interface (Bluetooth, Wifi)	4) ransomware attack 5) Bitcoin mining, etc															Anti-virus with updated virus definitions	2. SRS D001020024 - 2.17.6The	1) DSTC001: GSL-STC-001								
			(diuetooth, Wifi)																 Audit/System log capturing any abnormal activity identified/repo the application 	ted by anti-malware mechanism	2) DSTC001: GSL-STC-002								
T01	v	16 A	01		Low	Low L	w Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	the application 4. Use hardened interfaces (n/w) secure tunnel communications ch	& 3.SRS D001020024 -2.23.1 The innel Application shall have logs of table application and firmware	3) DSTC001: GSL-STC-003					#N/A	#N/	/A	
																				(SmartMedic devices).	4) DSTC001 - GSL-STC-004								
																				4. SRS D001020024 -2.17.2The Application shall provide secure									
16 Deliver un	indirected malware 185)	Unencrypted data in transit in all	Smart medic (Stryker device)	Malicious utilization of computer resources 2) computing	g power NA	+			+		+								LOW 1. Asset should be behind stateful	tunnel Communications channel	Penetration Testing Protocol	-		+ +					
(CAPEC-1	185]	flowchannels	System Component	3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc															firewall 2. Anti-virus with updated virus	Detection/Protection	Document #: D001020037: 1) DSTC001: GSL-STC-001								
T01	v	17 A	03	a, ancom mining, will	None	None H	gh Network	Low	High	None	Unchanged	12	0.6	3.6	4.9	Low	0.2	3.9	definitions 3. Audit/System log capturing any abnormal activity identified/repo		NA					#N/A	#N/	/A	
																			the application 4. Use hardened interfaces (n/w)	&									
				-					-	-	_								secure tunnel communications ch	nunc.	-				-				

Stepher Canadaminal

			Adverse Impact										Pre-Implementation of S	ecurity Controls							S	ecurity Controls/Mitigations						Post-Implement	tation of Security Controls		
# Threat Event(s)	Vulnerabilities	Asset	Impa	t Description	Safety Impact (Risk ID# or N/A)	ifidentiality	Integrity vallability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Sco	re ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures	Implementation of Risk Contr Measures	verification of Risk Contro Measures (Effectiveness)	ofidentiality integrity	Atta	ack Vector Attack Complexity	Privileges Required I	User Interaction	Scope CVSS v3.0 Base Score	Overall Risk Sec Score	urity Risk Residual Security Risk Ac Level Justification
17 Deliver undirected malware (CAPEC-185)	Unencrypted data in transit in all flowchannels	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet	denial of service attacks, ansomware attack	puter resources 2) computing power	ver NA	ā	<													fire 2. A	rwall Anti-virus with updated virus	1. SOM D001020115 - 23. Malwar Detection/Protection 2. SRS D001020024 - 2.17.6The	e Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001	8 -							
T01	/17	Application, Network interface (Bluetooth, Wifi)	s S) Bitcoin mining, etc			None	None High	Network	Low	High	None	Unchanged	1.2	0.6	36	49	Low	0.2	3.9	3. A abo the 4. U	Audit/System log capturing any normal activity identified/reported by application Use hardened interfaces (n/w) &	Application shall support the use anti-malware mechanism 3.SRS D001020024 - 2.23.1 The	2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003						#N/A	#N/A	
																				sec	rure tunnel communications channel	Application shall have logs of tabl application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The	4) DSTC001 - GSL-STC-004								
18 Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Device Maintainence tool (Hardware/Software)	Malicious utilization of com denial of service attacks, ansomware attack	puter resources 2) computing power	ver NA															fire	Asset should be behind stateful	Application shall provide secure tunnel Communications channel Device maintainence tool not implemented/existing in the SM	Penetration Testing Protocol								
T01	/23	A05	5) Bitcoin mining, etc			Low	Low Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	41	Moderate	0.5	3.8	defi 3. A abo the	finitions Audit/System log capturing any normal activity identified/reported by application	platform.	1) DSTC001: GSL-STC-028						#N/A	#N/A	
19 Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Smart medic (Stryker device) System Component	Malicious utilization of com denial of service attacks, armsomware attack	puter resources 2) computing power	ver NA															LOW 1. A	rwall Anti-virus with updated virus	1. SOM D001020115 - 23. Malwar Detection/Protection	Document #: D001020037:								
701	/23	A03	5) Bitcoin mining, etc			Low	Low Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	41	Moderate	0.5	3.8	defi 3. A abs	finitions ludit/System log capturing any normal activity identified/reported by application Use hardened interfaces (n/w) &	2,3,4. SRS D001020025	1) DSTC001: GSL-STC-001 NA						#N/A	#N/A	
20 Deliver undirected malware (CAPEC-185)	Outdated - Software/Hardware	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interface	1) Malicious utilization of com 3) denial of service attacks, 4) ransomware attack 5) Ritroin mining etc. 5) Ritroin mining etc.	puter resources 2) computing power	ver NA															LOW 1. A fire	ure tunnel communications channel Asset should be behind stateful ewall Anti-virus with undated virus	1. SOM D001020115 - 23. Malwar Detection/Protection 2. SRS D001020024 - 2.17.6The	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001								
T01	/23	(Bluetooth, Wifi)	J Decom manag, etc.			Low	Low Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	41	Low	0.2	3.6	abo the	Audit/System log capturing any normal activity identified/reported by application Use hardened interfaces (n/w) &	Application shall support the use anti-malware mechanism 3.SRS D001020024 - 2.23.1 The	2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003						#N/A	#N/A	
																				sec		Application shall have logs of tabl application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The	4) DSTC001 - GSL-STC-004								
21 Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Lantone Workstylions and	Device Maintainence tool (Hardware/Software)	Malicious utilization of com denial of service attacks, armsomware attack	puter resources 2) computing power	wer NA															fire	Asset should be behind stateful ewall	Application shall provide secure tunnel Communications channel Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037:								Justification
T02	Laptops, Workstations, and Servers	A05	5) Bitcoin mining, etc			None	None High	Local	Low	High	Required	Unchanged	0.6	0.6	3.6	42	Moderate	0.50	3.9	LOW 3. A abo the	ludit/System log capturing any normal activity identified/reported by application Use hardened interfaces (n/w) &	pastoria.	1) DSTC001: GSL-STC-028						#N/A	#N/A	
22 Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and	Smart medic (Stryker device) System Component	denial of service attacks, ansomware attack	puter resources 2) computing power	ver NA															LOW 1. A		1. SOM D001020115 - 23. Malwar Detection/Protection	Document #: D001020037:								
T02	Servers /21	A03	5) Bitcoin mining, etc			None	None High	Local	Low	High	Required	Unchanged	0.6	0.6	3.6	42	Moderate	e.s	39	abo the 4. U	initions ludit/System log capturing any normal activity identified/reported by application Use hardened interfaces (n/w) &	2,3,4. SRS D001020025	1) DSTC001: GSL-STC-001 NA						#N/A	#N/A	
23 Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Secures	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interface.	denial of service attacks, ansomware attack	puter resources 2) computing power	ver NA															LOW 1. A fire 2. A	rwall Inti-virus with updated virus	1. SOM D001020115 - 23. Malwar Detection/Protection 2. SRS D001020024 - 2.17.6The	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001								
T02	/21	(Bluetooth, Wifi)				Low	Low Low	Local	Low	Low	Required	Unchanged	13	0.5	3.4	4.8	Low	0.2	3.7	3. A abo the 4. L	Audit/System log capturing any normal activity identified/reported by application	Application shall support the use anti-malware mechanism 3.SRS D001020024 - 2.23.1 The	2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003						#N/A	#N/A	
																				300		application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The	4) DSTC001 - GSL-STC-004								
24 Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Wireless Network device (Scop of HDO)	e 1) Malicious utilization of com 3) denial of service attacks, 4) ransomware attack	puter resources 2) computing power	ver NA				_								Moderate			LOW SON		Application shall provide secure tunnel Communications channel 1. SOM D001020115 - 23. Malwar Detection/Protection 2. SOM D001020115 - 05. Access	e Penetration Testing Protocol Document #: D001020037:								
25 Deliver directed malware (CAPEC-185)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices,	3) denial of service attacks	puter resources 2) computing power	wer NA	Low	Low Low	Physical	Low	Low	Required	Unchanged	0.5	us	34	39	Noon are	0.5	3.7	per	rmission list for any sensitive & encrypted data if present. Asset should be behind stateful	1. SOM D001020115 - 23. Malwar Detection/Protection	1) DSTC001: GSL-STC-001 1) DSTC001: GSL-STC-017						#N/A	#N/A	
(Removable USB, Tablet Application, Network interface (Bluetooth, Wifi)	4) ransomware attack 5) Bitcoin mining, etc																	det 3. A abo	Inti-virus with updated virus finitions ludit/System log capturing any normal activity identified/reported by	2. SRS D001020024 -2.17.6The Application shall support the use anti-malware mechanism	1) DSTC001: GSL-STC-001								
T02	/13	A01				Low	Low Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	39	Moderate	0.5	3.7	4.1	cure tunnel communications channel	3.SRS D001020024 - 2.23.1 The Application shall have logs of tabl application and firmware (SmartMedic devices).	3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004						#N/A	#N/A	
26 Deliver directed malware	Unprotected external USB Port	Smart medic app (Stryker Adm	in 1) Malicious utilization of com	puter resources 2) computing power	ver NA															LOW 1.A		4. SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel 1. SOM D001020115 - 23. Malwar	e Penetration Testing Protocol								
(CAPEC-185)	on the tablet/devices.	Web Application)	3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc																	fire 2. A defi 3. A	rwall Inti-virus with updated virus finitions	Detection/Protection 2. Using web app the admin can all to view the functionality of different controls.	Document #: D001020037: ble 1) DSTC001: GSL-STC-001								
702	/13	A11				Low	Low Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	39	Low	0.2	35	the 4. U	application Use hardened interfaces (n/w) & oure tunnel communications channel	platform. Admin app doesnt contr any of the system components. He	not ance 3) DSTC001: GSL-STC-019 form						#N/A	#N/A	
																						3.SRS D001020097 = 2.23.2The Application shall provide facility audit logs for storing the user acti details.	of vity						,		
																						4.SRS D001020097 -2.17.5The Application shall provide secure tunnel Communications channel									
27 Deliver directed malware (CAPEC-185)	External communications and exposure for communication channels from and to application and devices like tablet and smartmedic device.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interface (Bluetooth, Wifi)	denial of service attacks, ansomware attack	puter resources 2) computing power	wer NA															dev mei 2. A	Only stryker made/authenticated vices should communicate with smart dic device & tablet ksset should be behind stateful swall	SRS D001020024 - 2.17.8 - Only Stryker made/ authenticated devishould be able to communicate w SM device and tablet.	Penetration Testing Protocol lices Document #: D001020037: ith 1) DSTC001: GSL-STC-010								
T02	/02	A01				None	None High	Network	Low	High	Required	Unchanged	0.9	0.6	36	45	Moderate	0.5	41	3.1	Use secure tunnel communications annel	Detection/Protection 3. SRS D001020024 - 2.17.2The	e 2) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-004						#N/A	#N/A	
																						Application shall provide secure tunnel Communications channel									
28 Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of con 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	puter resources 2) computing power	ver NA															fire 2. A def	ewall Anti-virus with updated virus finitions	Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-028								
T02	/08	AOS				Low	Low Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	abo the 4. U	Audit/System log capturing any normal activity identified/reported by application Use hardened interfaces (n/w) & suppression of communications channel								#N/A	#N/A	
29 Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Smart medic (Stryker device) System Component	Malicious utilization of com denial of service attacks, ransomware attack Bitcoin mining, etc	puter resources 2) computing power	ver NA		Low Low								3.4		Low	0.2	3.8	fire 2. A defi	rwall Inti-virus with updated virus finitions	1. SOM D001020115 - 23. Malwar Detection/Protection	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001						#N/A		
						Low	Low Low	Local	Low	Low	None	Unchanged	1.8	uS	2.4	53	Low	0.2	38	abo the 4. U sec	normal activity identified/reported by application Use hardened interfaces (n/w) & sure tunnel communications channel		NA						#N/A	#N/A	
30 Deliver directed malware (CAPEC-185)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interface (Bluetooth, Wifi)	denial of service attacks, ansomware attack	puter resources 2) computing power	wer NA															LOW 1. A fire 2. A defi	ksset should be behind stateful swall Anti-virus with updated virus linitions ludit/System log capturing any	1. SOM D001020115 - 23. Malwar Detection/Protection 2. SRS D001020024 - 2.17.6The Application shall support the use	Document #: D001020037: 1) DSTC001: GSL-STC-001								
T02	ros	A01				Low	Low Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	abo the	normal activity identified/reported by application Use hardened interfaces (n/w) & cure tunnel communications channel	anti-malware mechanism 3.SRS D001020024 -2.23.1 The	2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003						#N/A	#N/A	
																						(SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure									
31 Deliver directed malware (CAPEC-185)	Unprotected network port(s) on network devices and connection points	Smart medic (Stryker device) System Component	Malicious utilization of com computing power denial of service attacks, armsomware attack	puter resources	NA															dev mei 2. A	Only Stryker/HDO authenticated vices should communicate with smart dic device & tablet ksset should be behind stateful	tunnel Communications channel 1. SRS D001020025 2. SOM D001020115 - 23. Malwar	Penetration Testing Protocol Document #: D001020037:								
т02	/12	A03	5) Bitcoin mining, etc			None	None High	Network	Low	High	None	Unchanged	1.2	0.6	36	4.9	Moderate	0.5	43	fire 3. U	ewall Use secure tunnel communications unnel		2) DSTC001: GSL-STC-001						#N/A	#N/A	
																							PAGE 1								

Stepher Cantalonnial

			Adverse Impact									Pre-Implementation of S	ecurity Controls								Security Controls/Mitigations					Post-Imple	mentation of Security Controls			
Threat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impac (Risk ID# or N/A)	dentiality	tegrity illability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Scor	re ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Security Ris	isk Control Measures	Implementation of Risk Control Verification of Risk Control Measures (Effectives	ontrol as a second	ogrity ilability	Attack Vector Co	Attack Privilege emplexity Required	ges User	Scope CVSS v3.0	Base Overall Risk Score	Security Risk Residual S	Security Risk Acceptabilit Justification
Deliver directed malware (CAPEC-185)	Unprotected network port(s) on	Tablet Resources - web cam,	Malicious utilization of computer resources	N/A)	Confie	Avai														be behind stateful	1. SOM D001020115 - 23. Malware Penetration Testing Prof	ocol	Avail		, , , , , , , , , , , , , , , , , , , ,					
(CAPEC-185)	network devices and connection points	microphone, OTG devices, Removable USB, Tablet Application, Network interfac (Bluetooth, Wifi)	2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc																definitions	th updated virus	Detection/Protection Document #: D00102003 2. SRS D001020024 - 2.17.6The Application shall support the use of									
то2	V12	A01	J ween mang, ee		None	None High	Network	Low	High	None	Unchanged	1.2	0.6	3.6	4.9	Low	0.2	3.9	abnormal activit the application 4. Use hardened	ity identified/reported by d interfaces (n/w) &	anti-malware mechanism 2) DSTC001: GSL-STC-00 3.SRS D001020024 -2.23.1 The 3) DSTC001: GSL-STC-00						#N/A	#N/A		
																			secure tunnel co	ommunications channel	Application shall have logs of tablet application and firmware (SmartMedic devices).									
																					4. SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel									
Deliver directed malware (CAPEC-185)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and	Smart medic app (Stryker Adn Web Application)	nin 1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks,	NA															configuration mo mentioned in the	nodel needs to be se installation manual	Using web app the admin can able to view the functionality of different components existing in the SM Penetration Testing Protocomment #: D00102003	37:								
	Servers		4) ransomware attack 5) Bitcoin mining, etc																information sour intelligence and	irces for threat I vulnerability	platform. Admin app doesnt control any of the system components. Hence the risk associated to the SM platform with admin web ano can be isnored.	19								
T02	V21	A11			None	None High	Local	High	High	Required	Unchanged	0.3	0.6	3.6	4.0	Moderate	0.5	3.8	and taking appro high-priority ites	opriate action for	2. SOM D001020115 - 23. Malware Detection/Frotection 3.RS D001020097 - 21.7.2 The application shall allow to 4) DSTC001: GSL-STC-02						#N/A	#N/A		
																			4. Never create/i personal details	s such as date of birth, I's or pet's name	The application shall allow to upgrade the tablet application. 4. SRS D001020097 · 2.1.2.4 · Never create/use credentials with personal	11								
																			J. J. J. S.		details such as date of birth, spouse, or child's or pet's name 5.SOM D001020115 - 23. Malware									
Deliver directed malware	InSecure Configuration for	Tablet Resources - web cam,	Malicious utilization of computer resources	NA NA																be behind stateful	Detection/Protection 1. SOM D001020115 - 23. Malware 1) DSTC001: GSL-STC-00	11								
(CAPEC-185)	Software/OS on Mobile Devices, Laptops, Workstations, and Servers	microphone, OTG devices, Removable USB, Tablet Application, Network interfac (Bluetooth, Wifi)	2) computing power 3) denial of service attacks, 4) ransonware attack 5) Bitcoin mining, etc																definitions	th updated virus	Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of 3) DSTC001: GSL-STC-00									
Т02	V21 /	A01	-,		Low	Low Low	Local	Low	Low	Required	Unchanged	13	0.5	3.4	48	Low	0.2	3.7	abnormal activit the application 4. Use hardened	ity identified/reported by d interfaces (n/w) &	anti-malware mechanism 4) DSTC001 - GSL-STC-0 3.SRS D001020024 -2.23.1 The						#N/A	#N/A		
																			secure tunnel co		Application shall have logs of tablet application and firmware (SmartMedic devices).									
																					4. SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel									
Deliver directed malware (CAPEC-18S)	Unencrypted data at rest in all possible locations	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfac	Malicious utilization of computer resources computing power denial of service attacks,	NA															firewall 2. Anti-virus with	be behind stateful th updated virus	1. SOM D001020115 - 23. Malware Detection/Protection Pocument #: D00102003									
		Application, Network interfac (Bluetooth, Wifi)	s 4) ransomware attack 5) Bitcoin mining, etc																	ty Identified /reported by	2. SRS D001020024 - 2.17.6The Application shall support the use of anti-malware mechanism 1) DSTC001: GSL-STC-00	12								
T02	V16 A	A01			Low	Low Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.20	3.8	LOW 4. Use hardened secure tunnel co	ommunications channel	3.SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware 3) DSTC001: GSL-STC-00						#N/A	#N/A		
																					(SmartMedic devices). 4. SRS D001020024-2.17.2The Application shall provide secure									
6 Deliver directed malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Tablet OS/network details & Tablet Application	Malicious utilization of computer resources computing power	NA									+						firewall	be behind stateful	1. SOM D001020115 - 23. Malware Detection/Protection Document #: D00102003	ocol 87:								
			3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc																definitions 3. Audit/System	th updated virus	2. SRS D001020024 - 2.17.6The Application shall support the use of anti-malware mechanism 2) DSTC001: GSL-STC-00	11								
т02	V16	A02			Low	Low Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	the application 4. Use hardened	d interfaces (n/w) &	3.SRS D001020024 -2.23.1 The 3) DSTC001: GSL-STC-00	13					#N/A	#N/A		
																					application and firmware (SmartMedic devices). 4. SRS D001020024 - 2.17.2The	04								
7 Deliver directed malware	Unencrypted data at rest in all	Smart medic ann (Stryker ådn	nin 1) Malicious utilization of computer resources	NA.															LOW 1. Identification		Application shall provide secure tunnel Communications channel	aral ara								
Deliver directed malware (CAPEC-185)	Unencrypted data at rest in all possible locations	Web Application)	min 1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack																storage and encr subsystem 2. Stateful firewa	ryption of storage	2. SOM D001020115 - 23. Malware 1) DSTC001: GSL-STC-00									
T02	W16	A11	5) Bitcoin mining, etc		Low	Low Low	Local	Low	Low	None	Unchanged	1.8		34	53	Low	0.2	3.8	containing sensit 4. Maintain accer	itive data at rest ess control (read/modify)	Detection/Protection 2) DSTC001: GSL-STC-00 3. SAD/SDD-D001020099-6.7 Security 3) DSTC001: GSL-STC-00						#N/A	#N/A		
						200	200.20	Low	224	140000	Unchanged	2.5		-				"	unencrypted dat	ta if present. cryption algorithm	4) DSTC001: GSL-STC-01	17								
																					control policy and management 5) DSTC001: GSL-STC-00 5. SAD/SDD-D001020099-6.7	16								
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerab	NA bilities.															firewall	th updated virus	Security 1. SOM D001020115 - 23. Malware Detection/Protection Penetration Testing Prot Document #: D00102003	17:								
																			definitions 3. Audit/System abnormal activit the application	n log capturing any ity identified/reported by	2. SRS D001020024 - 2.17.6The Application shall support the use of anti-malware mechanism 1) DSTC001: GSL-STC-00									
т03	V12	A02			None	None Low	Network	Low	Low	None	Unchanged	2.8	0.2	1.4	43	Low	0.2	2.0	4 Use hardened	d interfaces (n/w) & ommunications channel	3.SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware 4) DSTC001 - GSL-STC-0						#N/A	#N/A		
																					(SmartMedic devices). 4. SRS D001020024 - 2.17.2The									
9 Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection	Smart medic app (Stryker Adn Web Application)	nin 1) Obtain knowledge about system internals 2) Attempt to find attack vectors	NA NA									+						MEDIUM 1. Admin applica	ation can be accessed by	Application shall provide secure tunnel Communications channel 1. Have to be closed before DR-8 Penetration Testing Prot 2. SAD/SDD-D001020099-6.7 Document #: D0010200	ocol								
W. J. D.	network devices and connection points	,	3) Possibilities for exploitation of publicly known Vulnerab	bilities.															required 2. Data transfer b	between the admin	2. SAD/SDD-D001020099-6.7 Document #: D00102003 Security 1) DSTC001: GSL-STC-03									
																			components nee secured.	eds to be encrypted &	Application shall establish technical controls to mitigate the potential for compromise to the integrity and confidentiality of health data stored									
T03	V12	A11			None	Low High	Network	Low	High	None	Unchanged	1.2	0.7	42	55	Low	0.2	45	connection point and hardened. 4. Maintain acces	nts should be identified	on the product or removable media Since admin application shall be						#N/A	#N/A		
																			permission list to unencrypted dat 5. Stateful firewa	all	app and it shall have no open ports until there is explicit requirement. 4.SRS D001020097 : 2.25.1 2Application shall have the User									
																					Management Screen to configure and manage the users as per the roles.									
																					S. SOM D001020115 - 23. Malware Detection/Protection									
Gaining Access ([S]TRID[E])	Unprotected network port(s) on network devices and connection	Tablet Resources - web cam, microphone, OTG devices,	2) Attempt to find attack vectors	NA NA															firewall		1. SOM D001020115 - 23. Malware Detection/Protection Document #: D00102003	ocol 87:								
	points	Removable USB, Tablet Application, Network interfac (Bluetooth, Wifi)	Possibilities for exploitation of publicly known Vulnerales	bilities.															definitions 3. Audit/System	log capturing any	2. SRS D001020024 - 2.17.6The Application shall support the use of anti-malware mechanism 2) DSTC001: GSL-STC-00									
т03	V12	A01			None	Low None	Network	Low	Low	None	Unchanged	28	0.2	1.4	43	Low	0.20	2.0	the application LOW 4. Use hardened	d interfaces (n/w) &	3.SRS D001020024 -2.23.1 The Application shall have loss of tablet	13					#N/A	#N/A		
																					application and firmware (SmartMedic devices). 4. SRS D001020024 - 2.17.2The	04								
1 Gaining Access	Devices with default passwords	Authentication/Authorisation	1) Obtain knowledge about system internals	NA NA															1.During the acco	cess providing, if default	Application shall provide secure tunnel Communications channel 1. Have to be closed before DR-8 Penetration Testing Prof									
Gaining Access ([S]TRID[E])	needs to be checked for bruteforce attacks	method of all device(s)/app	Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerab	bilities.															password is prov changing the pas	wided then immediately issword is needed.	2 SRS D001020023-2.1.2.2 If the Hospital Code is valid then on 1) DSTC001- CSU-STC-02	19								
																			2. Require muiti- 3. Limit authenti Limiting) 4. Maintain Acce	ess Logs	pressing the PROCEED button, the application shall be validated by the invisible captcha 3) DSTC001: GSL-STC-02 3) DSTC001: GSL-STC-02									
																					SRS D001020097 - 2.1.2.6 The Application shall be validated by using invisible captcha during login. 5) DSTC001: GSL-STC-01	19								
Т03	V01	A04			Low	None High	Physical	Low	Low	None	Unchanged	0.7	0.7	42	4.9	Moderate	0.50	4.6	MEDIUM		3. SRS D001020097 = 2.1.2.1.1 Invalid email or password, only 3 attempts left. 6) DSTC001: GSL-STC-01						#N/A	#N/A		
																					SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4.SRS D001020097 - 2.23.2 The									
																					4.SRS D001020097 - 2.23.2 The Application shall provide facility of audit logs for storing the user activity details.									
-								1													1									

Stepher Canadaminal

			Adverse Impact								Pre-Implementation of Secu	rity Controls								Security Controls/Mitigations					Post-Implem	entation of Security	Controls		
ID # Threat Event(s) Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	egrity	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	,	Implementation of Risk Control Measures	Verification of Risk Control	lentiality agrity	Attack Vector	Attack Privilege Complexity Required	User Interaction	Scope	CVSS v3.0 Base	Overall Risk Security Risk Score Level	Residual Security Risk Acceptability
42 Gaining Access ([S]TRID[E])	Devices with default password needs to be checked for	ds Interface/API Communication		N/A) SE	Ĭ	Avai		Required							anuation	2010		Low	During the access providing, if default promoted is provided than immediately.	1. Have to be closed before DR-8	Penetration Testing Protocol	Confic	Avail	complexity required	Intraction		J.D.C	AUC LEVEL	jutination
(b) ramps)	heeds to occasional or broad-rock and broad-rock an	A07	Attemption to find attack ventions Possibilities for exploitation of publicly known Vulnerable	lew	w None	ow Physical	Low	Low	None	Unchanged	0.7	0.4	25	12	Low	02	27		changing the password is sneeded. Also ensure: Also ensur	Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 – 2.1.26 The Application shall be validated by using invisible captcha during login.	1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014						#N/A	ΦN/A	
43 Gaining Access	The commend of the co		D Obtain hands about a star (stars)	NA.						Ш								MEDITAL	1 16 2 1 10 2 10 10 10 10 10 10 10 10 10 10 10 10 10	1.Have to be closed before DR-8	7) DSTC001: GSL-STC-006 1) DSTC001: GSL-STC-033								
(STRED(E))	The password complexity or location southershifty. Like we present the passwords of the passwords. Vol 1	mathod of all device(s)/app A04	1) Obtain knowledge about yegyem internals 2) Atmepte for fact, wetters 3) Possibilities for exploitation of publicly known Vulnerable 2) Possibilities for exploitation of publicly known Vulnerable	NA.	se None	ligh total	Low	Low	Required	Unchanged	13	0.7	42	56	Low	02	45		logic credentals & MFA. Thes, strong parawed policies & management are 2. Require multi-factive adherication 3.1 Junia adherication attempts; (see Laminos) (see Lamin	2.85 DOI:100.023.11.2.11/s. Supplication visit delivers or present glack them or present glack per processing the PROCEED betton, the proposition shall be validated by the introfilder capitals as the processing the validated by the introfilder capitals and the validated by the processing of the validated by the processing of the validated by th	2) ISTC001: GSL-STC-024 3) ISTC001: GSL-STC-025 4) ISTC001: GSL-STC-009 5) ISTC001: GSL-STC-044 6) ISTC001: GSL-STC-031 7) ISTC001: GSL-STC-031 8) ISTC001: GSL-STC-036						σN/A.	ØN/A	
44 Gaining Access ([S]THID[E])	Checking authentication mode for possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks and bypass of the possible hacks are possible hacks are possible hacks are possible ha	es Authentication/Authorisation method of all device(s)/app	1) Often is knowledge about years internals: 2) Attempt to find extract vectors: 3) Possibilities for exploitation of publicly known Walner abit	NA Low	e Low	ow Physical	Low	Low	None	Unchanged	67	0.5	34	41	Low	62	36	LOW	iderage le transit to miligire rich of machine de la consideration protection attacks 2. Encrypt authentication data using non reverentile encrypte much so using a feet of the consideration of the consideration of dictionary attacks. J. Lind, out accounts after reaching a lost dictionary attacks. J. Lind, out accounts after reaching a distinct of the consideration of the consideration breat ferror stanks. J. Dipply generic error messages upon validation of credentials to miligane rick of account harvesting or ensularation.	be encrypted. \$2.50,700.001020999-6.7 Security \$2.50,700.001020999-6.7 Security \$2.50,700.00102099-6.7 Security \$2.50,700.00102099-6.7 Security \$2.50,700.00102099-7.2 Security \$2.50,700.001	2) ISTOROIL GSL-STC-006 3) ISTOROIL GSL-STC-006 4) ISTOROIC GSL-STC-009 5) ISTOROIC GSL-STC-009 6) ISTOROIL GSL-STC-019 7) ISTOROIL GSL-STC-015 8]ISTOROIL GSL-STC-015						sN/A	вмд	
45 Gaining Access ((STRED(E))	Checking authentication mode for possible hacks and hypasse with the control of t	es Smart melic app (Stryker Adm Web Application) All	in 1) Observation of the desired server internals 2) Observation for desired vectors 3) Possibilities for exploitation of publicly known Wilnerabi	NA Low	ee Low	ow Physical	Low	Low	None	Unchanged	67	0.5	3.6	41	Low	0.2	36	LOW	storage & transit to mitigate risk of midration discharger and sold and the storage of the control of 2. Biotype authentication data using non reversible encrypton such as using a digest (Eq., 1865)) and a wed prevent days of the control of the control of 3. Lock our accurate side resulting go on failure thresholds and mitigate risk of the likest authors of the likest authors of wild also also also wild also also wild also also wild also wild also wild also wild also wild also wild also wild also wild also wild	Remember me' feature for login credentials and all the data which we shall store inside local storage shall be encrypted. SAD/SDD-D001020099-6.7 Security 2-SAD/SDD-D001020099-6.7 Security 3. SRS D001020097-2.12.1.1	1) DSTC001: GSL-STC-012 2) DSTC001: GSL-STC-006 3) DSTC001: GSL-STC-006						#N/A	#N/A	
46 Gaining Access ([S]TRID[E]) T03	Checking authentication mode for possible hacks and bypasse vote	es Smart medic app (Asure Portal es Administrator)	1) Obtain knowledge about ygreen internals 2) Attempt to find stack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities	NA NA Low	w Low	ow Physical	Low	Low	None	Unchanged	0.7	0.5	24	a	Low	62	3.6	LOW	storage & transit to mitigate risk of information disclosure and		Document #: D001020037:						an/A	#N/A	
47 Gaining Access ((S)TNID(E)) T03	Unprotected external USB Por on the tables/ devices.	Tablet Resources - web cam, merophene, ITG devices, merophene, ITG devices, Application, Network interface (Bluetooth, Wiff) A01	Stein knowledge about yetem internals: Attempte for finantive victors: Pounthilizies for exploitation of publicly known Wulnerable Pounthilizies for exploitation of publicly known Wulnerable	NA Low	w Low	ow Physical	Low	Low	Required	Unchanged	0.5	0.5	24	19	Low	62	35	LOW	firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	SRS D001020024 - 2.17.6The Application shall support the use of anti-malware mechanism SRS D001020024 - 2.23.1 The	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003						sn/A	σN/A	
48 Maintaining Access (TTP)	Devices with default passwort needs to be chacked for brusteforce attacks	ds Authentication/Authorsuston method of all device(s)/app	Stead in Noverledge about system internals Attempts from facts divectors Possibilities for exploitation of publicly known Vulnerabit Possibilities for exploitation of publicly known Vulnerabit	NA littes.	se Low	ow Physical	Low	Low	None	Unchanged	0.7	0.5	24	a	Moderate	es	3.8	LOW	password is provided then innomitately theming the parametris reseted. The thought the parametris reseted to the parameters of the paramet	2.SKS D001020023-2.1.2.2 ff the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the Invisible captchs SKS D001020007 - 2.1.2.6 The Application shall be validated by using switche captchs of the property	2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014 6) DSTC001: GSL-STC-031 7) DSTC001: GSL-STC-031						#N/A	#N/A	
49 Maintaining Access (TTP) TO6	The password complexity or location value ability. Life we proceed the passwords and hardcoded apasswords.	Authentication/Authorisation method of all device(t)/app	Obtain knowledge about system internals Attempt in find attack venture Northintees the exploitation of publicly known Wilnerable Secretary and secretary systems of publicly known Wilnerable	NA.	se Lowe	ow Lacal	Low	Low	Required	Unchanged	13	0.5	14	u	Low	62	37	LOW	logic reconstration MAT. These, strong logic reconstration of the management of required and the cutter authentication 2. Require multi-factor authentication 2. Require multi-factor authentication 2. Regular authentication and the cutter page (special reconstration of factor), larged, page (special reconstration of factor), larged, 5. Sandriffyprism large - Maintain security logic (such as factor) modification of the cutter of the cutter page (such as factor) modification of the cutter of the cutter of the cutter of the cutter of the cutter of	2. SRS D0010200123-2.12.2 If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 - 2.12.6 The Application shall be validated by using invisible captcha during login. 3. SRS D001020097 - 2.12.1 Invalid	4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014 6) DSTC001: GSL-STC-031 7) DSTC001: GSL-STC-031						#N/A	en/A	

Stopher Grandsmit

Threat Event(s)												Pre-Implementation of Secu	urity Controls							Security Controls/Mitigations			Pe	it-Implementation of Security Control		
Inreat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impac (Risk ID# or	a p	egrity	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base In	mpact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Security Risk Control Measures	Implementation of Risk Control Measures Measures (Effectiveness)	dentiality	Attack Vec	Attack Privileges Complexity Required Inte	Jser Scope CVSS v3	D Base Overall Risk !	iecurity Risk Residual Security Risk Acceptability Level Justification
Clearing Track	InSecure Configuration for Software/OS on Mobile Devices,	Tablet Resources - web cam, microphone, OTG devices,	Tampering of forensic data This involves modifying/corrupting/deleting the values of	N/A)	Confic	Int			,										LOW 1. Asset should be behind stateful from: 11	1. SOM D001020115 - 23. Malware Penetration Testing Protocol Detection/Protection Document #: D001020037:	Confit	Avail				
(117)	Laptops, Workstations, and Servers	Removable USB, Tablet	3] Modifying registry values 4] Uninstalling all malcious applications/tools 5) Deleting all folders which were created	Llogs,															2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported b	2. SRS D001020024 - 2.17.6The 1) DSTC001: GSL-STC-001 Application shall support the use of						
т05	V21	A01			Low	Low Low	Local	Low	Low	Required	Unchanged	13	0.5	3.4	48	Low	0.2	3.7	the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	3.SRS D001020024 -2.23.1 The 3) DSTC001: GSL-STC-003 Application shall have loss of tablet				an	A #N/A	
																				(SmartMedic devices). 4. SRS D001020024 - 2.17.2The						
Clearing Track (TTP)	Outdated - Software/Hardware	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet	Tampering of forensic data This involves modifying/corrupting/deleting the values of all Modifying registry values	B- L2(Reference	e						\vdash								LOW 1. Asset should be behind stateful firewall	Application shall provide secure tunnel Communications channel 1. SOM D001020115 - 23. Malware Detection/Protection Document #: D001020037:						
		Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Modifying registry values Uninstalling all malcious applications/tools Deleting all folders which were created	and Risk Matrix SmartMedic																2. SRS D001020024-2.17.6The Application shall support the use of y anti-malware mechanism 2) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002						
т05	V23	A01		Document # D001020010)) Low	Low Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	41	Moderate	0.5	3.8	the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	3.SRS D001020024-2.23.1 The Application shall have logs of tablet application and firmware 4) DSTC001- GSL-STC-004				an	A #N/A	
																				(SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure						
Clearing Track (TTP)	Lack of configuration controls for IT assets in the information system plan	Tablet Resources - web cam, microphone, OTG devices, Removable USB. Tablet	Tampering of forensic data This involves modifying/corrupting/deleting the values of Modifying registry values	B- L2(Reference Risk Table	e														LOW 1. Asset should be behind stateful firewall 2. Anti-virus with updated virus	tunnel Communications channel 1. SOM D001020115 - 23. Malware Detection/Protection Penetration Testing Protocol Document #: D001020037:						
	7,	Application, Network interfaces (Bluetooth, Wifi)	Modifying registry values Uninstalling all malcious applications/tools Deleting all folders which were created	and Risk Matrix SmartMedic Document #															definitions 3. Audit/System log capturing any abnormal activity identified/reported b the application	2. SRS D001020024 - 2.17.6Tbe Application shall support the use of y anti-malware mechanism 2) DSTC001: GSL-STC-002						
T05	V07	A01		D001020010))) Low	Low Low	Local	Low	Low	Required	Unchanged	13	0.5	3.4	48	Low	0.2	3.7	4. Use hardened interfaces (n/w) &	3.SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4) DSTC001 - GSL-STC-004				an	A #N/A	
																				4. SRS D001020024 - 2.17.2The Application shall provide secure						
Clearing Track (TTP)	Lack of configuration controls for IT assets in the information system plan	Device Maintainence tool (Hardware/Software)	Tampering of forensic data This involves modifying/corrupting/deleting the values of Modifying registry values Uninstalling all malcious applications/tools	B- L2(Reference Risk Table and Risk	e														1. Asset should be behind stateful firewall 2. Anti-virus with updated virus	tunnel Communications channel Device maintainence tool not						
т05	V07	A05	Uninstailing all malcious applications/tools Deleting all folders which were created	Matrix SmartMedic Document #		Low Low	Local	Low	Low	Required	Unchanged	13	0.5	3.4	48	Low	0.2	3.7	aennitions 3. Audit/System log capturing any abnormal activity identified/reported b the application	1) DSTC001: GSL-STC-028				an	A #N/A	
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications	Tablet Resources - web cam, microphone, OTG devices,	Tampering of forensic data This involves modifying/corrupting/deleting the values of	D001020010) B- L2(Reference	_						Н								Use hardened interfaces (n/w) & secure tunnel communications channel 1. Asset should be behind stateful firewall	1. SOM D001020115 - 23. Malware Detection/Protection Penetration Testing Protocol Document #: D001020037:						
	thoughout the information system plan	Removable USB, Tablet	Modifying registry values Uninstalling all malcious applications/tools Deleting all folders which were created	Risk Table and Risk Matrix SmartMedic															Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by	2. SRS D001020024-2.17.6The Application shall support the use of anti-malware mechanism 2) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002						
т05	V08	A01		Document # D001020010)	None None	Low Low	Local	Low	High	None	Unchanged	8.0	0.4	25	3.4	Moderate	0.5	3.0	the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	3.SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4) DSTC001 - GSL-STC-004				αN	A #N/A	
																				4. SRS D001020024 - 2.17.2The Application shall provide secure						
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information	Device Maintainence tool (Hardware/Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of 3) Modifying registry values	Risk Table	e						П								1. Asset should be behind stateful firewall 2. Anti-virus with updated virus	tunnel Communications channel Device maintainene tool not Penetration Testing Protocol implemented/existing in the SM platform. Document #: D001020037:						
т05	system plan	A05	4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	and Risk Matrix SmartMedic Document #	Low	Low Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application	1) DSTC001: GSL-STC-028				an	A #N/A	
				D001020010)	0)						Ш								 Use hardened interfaces (n/w) & secure tunnel communications channel 							
Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	Tablet OS/network details & Tablet Application	Tampering of forensic data This involves modifying/corrupting/deleting the values of 3 Modifying registry values Uninstalling all malcious applications/tools	and Risk	e														1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions	1. SOM D001020115 - 23. Malware Penetration Testing Protocol Document #: D001020037: 2. SRS D001020024 - 2.17.6Tbe 1) DSTC001: GSL-STC-001						
T05	vos	A02	S) Deleting all folders which were created	Matrix SmartMedic Document #) Low	Low Low	Local	Low	Low	None	Unchanged	1.8	05	3.4	53	Low	0.2	3.8	Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) &	Application shall support the use of anti-malware mechanism 2) DSTC001: GSL-STC-002				an	A #N/A	
												_			_		_		secure tunnel communications channel	Application shall have logs of tablet application and firmware (SmartMedic devices). 4) DSTC001 - GSL-STC-004 (SmartMedic devices).						
Classics Touch	The static connection digaram	Davies Majories and	D7-marks of formula data	D.							Ш								LOW 1. Asset should be behind stateful	4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel Device maintainence tool not 1) DSTC001: GSL-STC-028						
Clearing Track (TTP)	between devices and applications with provision for periodic updation as per changes	Device Maintainence tool (Hardware/Software)	Timpering of forensic data This involves modifying/corrupting/deleting the values of Modifying registry values Uninstalling all malcious applications/tools	L2(Reference Risk Table and Risk	e														firewall 2. Anti-virus with updated virus definitions	Device maintainence tool not implemented/existing in the SM platform.						
т05	V10	A05	5) Deleting all folders which were created	Matrix SmartMedic Document # D001020010]	Low	Low Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	53	Low	0.2	3.8	 Audit/System log capturing any abnormal activity identified/reported b the application Use hardened interfaces (n/w) & 	,				an	A #N/A	
																			secure tunnel communications channel							
Clearing Track (TTP)	The static connection digaram between devices and applications with provision for	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet	Tampering of forensic data This involves modifying/corrupting/deleting the values of Modifying registry values Holinstalling all malcious applications/tools	B- L2(Reference Risk Table	e														1. Asset should be behind stateful firewall 2. Anti-virus with updated virus	1. SOM D001020115 - 23. Malware Detection/Protection Penetration Testing Protocol Document #: D001020037: 2. SRS D001020024 - 2.17.6Tbe 1) DSTC001: GSL-STC-001						
	periodic updation as per changes	(Bluetooth, Wifi)	Uninstailing all malcious applications/tools Deleting all folders which were created	SmartMedic Document #															definitions 3. Audit/System log capturing any abnormal activity identified/reported b the application	Application shall support the use of anti-malware mechanism 2) DSTC001: GSL-STC-002						
105	V10	A01		D001020010])) Low	Low Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	 Use hardened interfaces (n/w) & secure tunnel communications channel 	3.SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 3) DSTC001: GSL-STC-003 Application and firmware (DSL-STC-004 (SmartMedic devices).				an	A #N/A	
																				4. SRS D001020024-2.17.2The Application shall provide secure						
Elevation of privilege (STRID(E])	Controlled Use of Administrative Privileges over the network	Authentication/Authorisation method of all device(s)/app	Gaining access to the portal Accessing confidential data, Accessing on onlidential data Company defamation Company defamation	NA															1. Require that administrators establish multi factor authentication for their administrator and non-administrative accounts.	1.SRS D001020023-2.1.2.2 if the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the 11 DSTC001: GSL-STC-024						
			T) Company desimation																 Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. 	Invisible captcha SRS D001020097 = 2.1.2.6 The 2) DSTC001: GSL-STC-025						
T06	VIS	AD4			Low	Low Low	Network	Low	Low	Required	Unchanged	2.1	0.5	3.4	5.5	Low	0.2	3.8	 Ensure default credentials not existin for any assets (such as applications, operating systems, routers, firewalls, wireless access points). 	using invisible captcha during login 3) DSTC001: GSL-STC-026 2. SAD D001020032 5.3 TCP/IP 4) DSTC001: GSL-STC-029				#N	A #N/A	
																				Communication 3. Have to be closed before DR-8						
Elevation of privilege (STRID[E])	Controlled Use of Administrative Privileges over the network	Smart medic app (Azure Portal Administrator)	Accessing confidential data, Lead misuse of confidential data	NA															MEDIUM 1. Require that administrators establish multi factor authentication for their administrator and non-administrative	The setup & configuration process of azure cloud & admin shall be document #: D001020037:						
T06	V15	A12	4) Company defamation		None	Low High	Network	Low	High	Required	Unchanged	0.9	0.7	42	5.2	Moderate	0.5	47	2. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts.					an	A #N/A	
																			 Ensure default credentials not existin for any assets (such as applications, operating systems, routers, firewalls, wireless access points). 	5						
Denial of service (STRI(D)E)	Unprotected network port(s) on network devices and connection points	Tablet OS/network details & Tablet Application	Bring down the service availability Blocking the end user usage	NA NA							+									SOM D001020115 - 23. Malware Detection/Protection Document #: D001020037:						
	points																		definitions 3. System log capturing any abnormal activity identified/reported by the	2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 2) DSTC001: GSL-STC-002						
Т07	V12	A02			None	None High	Network	Low	Low	None	Unchanged	2.8	0.6	3.6	6.5	Low	0.2	42	application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	3.SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware 3) DSTC001: GSL-STC-003				an	A #N/A	
																				(SmartMedic devices). 4) DSTC001 - GSL-STC-004 4. SRS D001020024 -2.17.2The Application shall provide secure						
Information disclosure (STR(I)DE)	Unencrypted data at rest in all possible locations	Data at Rest	Information of health data can be exploit and disclose with va means like network, tablet etc	arious NA	+ +														1. Identification of the sensitive data in storage and encryption of storage subsection.	tunnel Communications channel 1. SRS D001020097 - 2.1.2.3The Application shall have the Document #: D001020037:						
																			subsystem 2. Stateful firewall 3. Hardening of the host system containing sensitive data at rest	"Remember me' feature for login credentials and all the data which we shall store inside local storage shall be encrypted. 2) DSTC001: GSL-STC-001						
																			4. Maintain access control (read/modif	2. SOM D001020115 - 23. Malware Detection/Protection 4) DSTC001: GSL-STC-008						
T08	V16	A09			Low	Low Low	Local	High	High	None	Unchanged	0.5	0.5	3.4	39	Moderate	0.5	3.7		3. SAD/SDD-D001020099-6.7 Security 5) DSTC001: GSL-STC-006 4. SRS D001020097 : 2.25.1				an	A #N/A	
																				Application shall have the User Management Screen to configure and manage the users as per the roles.						
			1																	5.SAD/SDD-D001020099-6.7 Security						

				Adverse Impact																							mentation of Security Controls			
ID# T	Threat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	lentiality	egrity lability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base In	spact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	lentiality grity	Attack Vector	Attack Privil Complexity Requi	leges User	Scope CVSS v3.0 B	ase Overall Risk	Security Risk Residual Securit	ty Risk Acceptability
63 Informa (STR(1)	ation disclosure (DE)	Unencrypted data in transit in all flowchannels	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc		Confi	Int Avai													LOW 1. Use secure tunnel communication channel	1.SRS D001020024 -2.17.2The Application shall provide secure	Penetration Testing Protocol Document #: D001020037:	Confi	Avai	y		Jole		Just	
																				 Configure and upgrade routers for the n/w security Configure firewalls to reject any packets with spoofed addresses. 	e tunnel Communications channel SRS D001020023 - 2.13.3The Application shall provide secure tunnel Communications channel	1) DSTC001: GSL-STC-004 2) DSTC001: GSL-STC-004								
тов	v	/17 A1	10			Low	None Low	Network	High	Low	None	Unchanged	1.6	0.4	25	42	Moderate	0.5	3.4	Maintain access control (read/modif permission list for any sensitive & unencrypted data if present. S. For sensitive data proper encryption	2. SOM D001020115 - 16. Transmission confidentiality and integrity	3) DSTC001: GSL-STC-016 4) DSTC001: GSL-STC-001					#N/A	#N/A		
																				mechanism needs to be designed & implemented	3. SOM D001020115 - 23. Malware Detection/Protection	5) DSTC001: GSL-STC-017								
																					SOM D001020115 - 05. Access control policy and management S.SAD/SDD-D001020099-6.7	6) DSTC001: GSL-STC-006								
64 Informa (STR(I)	ation disclosure (DE)	Weak Encryption Implementation in data at rest and in transit tactical and design wise	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc	us NA															LOW 1. Implement server-side encryption using Service-Managed keys/recomended practise by azure.	Cloud Infrastructure	Penetration Testing Protocol Document #: D001020037:								
																				for ex: when files are moved to cloud storage, etc	it, control policy and management	1) DSTC001: GSL-STC-020 2) DSTC001: GSL-STC-017								
																				Transfer over encrypted tunnel Use strong encryption algorithm	Security Tablet-SDD-D001020040-6.7- Security NSA-SAD-D001020031-6.7-Security	3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-006 5) DSTC001: GSL-STC-006								
тов	v	/18 AC	.09			Low	Low Low	Local	High	High	None	Unchanged	0.5	0.5	3.4	39	Moderate	0.5	3.7		SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel	6) DSTC001: GSL-STC-004					#N/A	#N/A		
																					SRS D001020023- 2.13.3The Application shall provide secure tunnel Communications channel	7) DSTC001: GSL-STC-004 8) DSTC001: GSL-STC-021								
																					NSA-SDD-D001020110-4.2.1-Nurse Station Web Services	9) DSTC001: GSL-STC-006								
																					5. NSA-SAD-D001020031-6.7- Security									
65 Informa (STR(I)	ation disclosure (DE)	Weak Encryption Implementation in data at rest and in transit tactical and design wise	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	us NA															Statefull firewall Configure and upgrade routers for the n/w security Configure firewalls to reject any	1. SOM D001020115 - 23. Malware Detection/Protection 2. SOM D001020115 - 16.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001								
																				packets with spoofed addresses. 4. Use secure tunnel communication channel	Transmission confidentiality and	2) DSTC001: GSL-STC-016								
TOS	, v	718	10			Low	None Low	Network	High	Low	None	Unchanged	1.6	0.4	25	42	Moderate	0.5	3.4		Detection/Protection 4. SRS D001020024 - 2.17.2The Application shall provide secure	3) DSTC001: GSL-STC-001					#N/A	#N/A		
																					tunnel Communications channel	4) DSTC001: GSL-STC-004					,	,-		
	ation disclosure	Weak Algorthim implementation	Data at Rest	Information of health data can be exploit and disclose with various	us NA															LOW 1. Weak algorithms such as DES, RC4.	1. SRS D001020097 -2.8.1Applicatio	on Penetration Testing Protocol								
(STR(I)	(DE)	with respect cipher key size		means like network, tablet etc																etc should be avoided and usage of strong algorithms such as AES, RSA, etc are recomended 2. Tunical loss longths are 129 and 254.	shall use APIs to communicate between browser application and th backend.	Document #: D001020037: ne 1) DSTC001: GSL-STC-011								
T08	V	719 AC	09			Low	Low Low	Local	High	High	None	Unchanged	0.5	0.5	3.4	39	Moderate	0.5	3.7	bits for private keys and 2048 for public keys are recommended.	c 2. SRS D001020097 – 2.8.1Applicatic shall use APIs to communicate between browser application and th backend.	ne 2) DSTC001: GSL-STC-011					#N/A	#N/A		
	ation disclosure	Weak Algorthim implementation	Data in Transit	Information of health data can be exploit and disclose with various	us NA															LOW 1. Weak algorithms such as DES, RC4,	1. SRS D001020097 -2.8.1Applicatio	on Penetration Testing Protocol								
(STR(I)	(DE)	with respect cipher key size		means like network, tablet etc																1. Weak algorithms such as DES, RC4, etc should be avoided and usage of strong algorithms such as AES, RSA, etc. are recomended 2. Typical key lengths are 128 and 256	backend.	1) DSTC001: GSL-STC-011								
тов	V	719 A1	10			Low	None Low	Network	High	Low	None	Unchanged	1.6	0.4	25	4.2	Moderate	0.5	3.4	bits for private keys and 2048 for public keys are recommended.	c 2. SRS D001020097 – 2.8.1Applicatic shall use APIs to communicate between browser application and th backend.						#N/A	#N/A		
68 Informa	ation disclosure	InSecure Configuration for	Tablet Resources - web cam,	Information of health data can be exploit and disclose with various	us NA															LOW 1. Asset should be behind stateful	1. SOM D001020115 - 23. Malware	Penetration Testing Protocol Document #: D001020037:								
(STR(I)	(DE)	Insecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	means like network, tablet etc																firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any	2.SRS D001020024 - 2.17.6The Application shall support the use of	Document #: D001020037: 1) DSTC001: GSL-STC-001								
тов	v	721 A	101			Low	Low Low	Network	High	High	None	Unchanged	0.7	0.5	3.4	41	Moderate	0.5	3.8	abnormal activity identified/reported by the application identified/reported by the application 4. Use hardened interfaces (n/w) &	3.SRS D001020024 - 2.23.1 The Application shall have logs of tablet	2) DSTC001: GSL-STC-002					#N/A	#N/A		
																				secure tunnel communications channel	(SmartMedic devices).	3) DSTC001: GSL-STC-003								
																					4. SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel	4) DSTC001 - GSL-STC-004								
69 Informa (STR(I)	ation disclosure (DE)	Unencrypted Network segment through out the information flow	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	us NA															1. Anonymization/Pseudomyzation of patient details 2. Data encyrption 3. Audit/System log - Maintain Access logs (login (attempted & failed), logoff,	application shall allow to assign and	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-005								
																				change) 4. Audit/System log - Maintain security logs (such as change/modification of	Security Tablet-SDD-D001020040-6.7- Security	2) DSTC001: GSL-STC-006 3) DSTC001: GSL-STC-006								
тов	v	/14 A	110			Low	None Low	Network	High	Low	None	Unchanged	1.6	0.4	25	42	Moderate	0.5	3.4	system configuration settings, services, etc.)	NSA-SAD-D001020031-6.7-Security 3.SRS D001020024-2.23.1 The Application shall have logs of tablet	4) DSTC001: GSL-STC-006					#N/A	#N/A		
																					application and firmware (SmartMedic devices).	6) DSTC001: GSL-STC-003								
																					4.SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices).									
70 Informa (STR(I)	ation disclosure (DE)	Insecure communications in networks (hospital)	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	us NA															1. Secure communication with Secure Sockets Layer (SSL) or TLS protocols the provide message confidentiality 2. Secure sensitive data in the channel	SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-004								
																				flow using strong encryption 3. Statefull firewall 4. Proper way of network access contro	2. SAD/SDD-D001020099-6.7 Security									
TOS	, v	705 A	110			Low	None Low	Network	High	Low	None	Unchanged	1.6	0.4	25	42	Moderate	0.5	3.4		Solve Debricorins - 23. Stateware Detection/Protection 4. SOM D001020115 - 05. Access control policy and management	3) DSTC001: GSL-STC-001					zn/a	#N/A		
																					control pointy and management	4) DSTC001: GSL-STC-017					,	,-		
71 Data Ac	ccess	Unprotected network port(s) on	Tablet Resources - web cam.	Allowing application or script to perform abnormal activites on	n NA															LOW 1. Asset should be behind stateful	1. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol								
71 Data Ac (STR[I])	DE)	Unprotected network port(s) on network devices and connection points	microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Allowing application or script to perform abnormal activities on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.																Anti-virus with updated virus definitions Audit/System log capturing any	2.SRS D001020024 - 2.17.6The Application shall support the use of	1) DSTC001: GSL-STC-001								
T09	v	V12 A	101			None	None High	Network	High	High	None	Unchanged	0.7	0.6	36	44	Low	0.2	3.8	abnormal activity identified/reported b the application 4. Use hardened interfaces (n/w) &	anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have loss of tablet	2) DSTC001: GSL-STC-002					#N/A	#N/A		
																					application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The	4) DSTC001 - GSL-STC-004								
72 Data Ac	ccess	Unprotected network portfs) on	Tablet OS/network details &	Allowing application or script to perform abnormal activities on	on NA															LOW 1. Asset should be behind stateful	Application shall provide secure tunnel Communications channel 1. SOM D001020115 - 23. Malware	Penetration Testing Protocol								
72 Data Ac (STR[I]I	DE)	Unprotected network port(s) on network devices and connection points	Tablet Application	2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.																firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any	2.SRS D001020024 - 2.17.6The Application shall support the use of	Document #: D001020037: 1) DSTC001: GSL-STC-001								
T09	v	V12 A	102			None	Low Low	Network	High	High	None	Unchanged	0.7	0.4	25	33	Low	0.2	2.7	abnormal activity identified/reported to the application 4. He hardened interfaces (n/w) &	anti-malware mechanism	2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003					#N/A	#N/A		
																					Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The	4) DSTC001 - GSL-STC-004								
																					Application shall provide secure tunnel Communications channel									

Stepher Canadaminal

			Adverse Impact									Pre-Implementation of S	Security Controls								Security Controls/Mitigations				Post-Implen	mentation of Security Controls			
ID # Threat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	dentiality	tegrity ilability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Sco	re ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Security Risk Con	trol Measures	Implementation of Risk Control Verification of Risk Control Measures (Effectivenes	dentiality (s	lability	Attack Vector Attack Privilege: Complexity Required	User Interaction	Scope CVSS v3.0 Base Score	Overall Risk Score	Security Risk I	Residual Security Risk Acceptability Justification
73 Data Access (STR[I]DE)	Devices with default passwords needs to be checked for	Data at Rest	Allowing application or script to perform abnormal activites on the system.		Confi	In Ava													LOW 1. During the access p	then immediately	1. Have to be closed before DR-8 Penetration Testing Protoco Document #: D001020037:	9 1	Avai						
	bruteforce attacks		Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.																changing the passwor Also ensure: 2. Statefull firewall 3. Do not store sensiti	l is needed.	2. SOM D001020115 - 23. Malware Detection/Protection 1) DSTC001: GSL-STC-029 3. SAD/SDD-D001020099-6.7								
																			Use strong encrptio Apply salting over s	n algorithm. ensitive data.	Secrurity SRS D001020023-2.13.2System shall store patient id in anonymized fashion. 3) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-006								
																					4.SAD/SDD-D001020099-6.7 Security 4) DSTC001: GSL-STC-013 5.SAD/SDD-D001020099-6.7 Security								
Т09	V01	A09			Low	Low Low	Network	High	High	None	Unchanged	0.7	0.5	3.4	41	Low	0.2	3.6			SRS D001020023-2.13.2System shall store patient id in anonymized fashion. 5) DSTC001: GSL-STC-006					#N/A	#N/A		
																					6) DSTC001: GSL-STC-006 7) DSTC001: GSL-STC-013								
74 Data Access (STR[i]DE)	Devices with default passwords needs to be checked for bruteforce attacks	Authentication/Authorisation method of all device(s)/app	Allowing application or script to perform abnormal activites or the system. Modifying the data, tampering the confidential data making it	on NA															1. During the access p password is provided changing the passwor Also ensure:	then immediately is needed.	2. SOM D001020115 - 23. Malware	d							
			unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)																Statefull firewall Do not store sensiti	e data in plaintext.	Detection/Protection 1) DSTC001: GSL-STC-029 3. SAD/SDD-D001020099-6.7 Security SRS D001020023-2:13.2System shall								
T09	VOI	404			High	None None	Network	High	High	None	Unchanged	0.7	0.6	36	44	Moderate	0.5	4.0	S. Apply salting over s		store patient id in anonymized fashion. 3) DSTC001: GSL-STC-006					#N/A	#N/A		
					1101	Attack Attack	ALTHOU &		1494	. Tools	Unchanged	2					2				4.SAD/SDD-D001020099-6.7 Security 4) DSTC001: GSL-STC-013 S.SAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.25ystem shall					TA/A			
																					store patient id in anonymized fashion. 5) DSTC001: GSL-STC-006 fashion. 6) DSTC001: GSL-STC-006								
75 Data Access	Devices with default passwords	Data in Transit	Allowing application or script to perform abnormal activites or	on NA															LOW 1. During the access p	oolding if dafruit	7) DSTC001: GSL-STC-013 1. Have to be closed before DR-8 Penetration Testing Protoco								
(STR[I]DE)	needs to be checked for bruteforce attacks	Arthur tot a tanada.	the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.																password is provided changing the passwor Also ensure-	then immediately is needed.	2. SOM D001020115 - 23. Malware Detection/Protection 1) DSTC001-GSL-STC-029								
			Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)																2 Statehul firewali 3 Do not store sensitiv 4. Use strong encrptio 5. Apply salting over s	n algorithm. ensitive data.	3. SAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.2System shall								
Т09	V01	A10			High	None None	Network	High	High	None	Unchanged	0.7	0.6	3.6	44	Low	0.2	3.8			store patient id in anonymized fashion. 3) DSTC001: GSL-STC-006 4.SAD/SDD-D001020099-6.7 Security 4) DSTC001: GSL-STC-013					#N/A	#N/A		
																					SSAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.2System shall store patient id in anonymized 5) DSTC001: GSL-STC-006								
																					fashion. 6) DSTC001: GSL-STC-006								
76 Data Access (STR[I]DE)	The password complexity or location subscrability. Like weak	Data at Rest	Allowing application or script to perform abnormal activites or the system.	on NA															LOW 1. Strong password str	ength practices is	7) DSTC001: GSL-STC-013 1. Have to be closed before DR-8 Penetration Testing Protoc: 2. SRS 00010/20073-2.1.2.2 lifthe Document #: 00010/20037-	d							
(311(1)05)	location vulnerability. Like weak passwords and hardcoded passwords.		2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (redeemtial/pins/MFA/Blometrics)																3. Limit authentication	attempts (rate	2. SRS D001020023-2.1.2.2 if the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captors.								
			(resembly least on st moments)																logs (login (attempted change) 5. Audit/System log -	& failed), logoff, id faintain security	SRS D001020097 - 2.1.2.6 The Application shall be validated by 3) DSTC001: GSL-STC-025								
т09	vas	A09			Low	Low Low	Network	High	High	None	Unchanged	0.7	0.5	3.4	41	Low	0.2	3.6	logs (such as change/s system configuration etc.) 6. Stronger authentica	ettings, services,	using Invisible captcha during login. 4) DSTC001: GSL-STC-009 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left.					#N/A	#N/A		
																					SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 6) DSTC001: GSL-STC-031 7) DSTC001: GSL-STC-031								
																					4. SRS D001020097 - 2.23.2 - Audit logs S. SRS D001020097 - 2.23.2 - Audit 8) DSTC001: GSL-STC-006 logs								
																					6. SAD/SDD-D001020099-6.7 Security								
77 Data Access (STR[I]DE)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet	Allowing application or script to perform abnormal activities or the system. System. System and the data, tampering the confidential data making it sunavailable or challenging the integrity of data. System or challenging the integrity of data.	on NA															1. Asset should be beh firewall 2. Anti-virus with upd		1. SOM D001020115 - 23. Malware Penetration Testing Protoco Document #: D001020037: 2. SRS D001020024 - 2. 17.6 The 1) DSTC001: GSL-STC-001	d							
		(Bluetooth, Wifi)	3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)																the application	tified/reported by	Application shall support the use of anti-malware mechanism 2) DSTC001: GSL-STC-002								
т09	V13	A01			None	Low Low	Physical	High	High	None	Unchanged	0.2	0.4	25	2.7	Moderate	0.5	26	4. Use hardened inter secure tunnel commu	ications channel	3SRS D001020024 -2 23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 3) DSTC001: GSL-STC-003					#N/A	#N/A		
																					4. SRS D001020024 -2 17.2The Application shall provide secure								
78 Open network port expl	oit Unprotected network port(s) on network devices and connection	Tablet OS/network details & Tablet Application	Capture your account's user ID and credentials. Dog the data of online traffic accessed on your tablet or comput	NA uter.															LOW 1. Asset should be beh firewall	ind stateful	tunnel Communications channel 4) DSTC001 - GSL-STC-004 1. SOM D001020115 - 23. Malware Detection/Protection Document #: D001020037:								
	points	,	In this way, they can maintain a data of the websites you mostly v and plan attack from these websites. 3) Gain access to your computer, its network and data. 4) Launch a spam or malware attack on your device.	visit,															Anti-virus with upd definitions Audit/System log co	pturing any	2-SRS D001020024-2-17.6The Application shall support the use of anti-malware mechanism								
Т10	V12	A02	4) Laurent apart of marvare access on your service.		None	None Low	Network	High	Low	None	Unchanged	1.6	0.2	1.4	31	Moderate	0.5	23	the application	bres (n/w) &	3.SRS D001020024-2.23.1 The Application shall have logs of tablet application and firmware					#N/A	#N/A		
																					(SmartMedic devices). 3) DSTC001: GSL-STC-003								
																					4. SRS D001020024-2.17.2The Application shall provide secure tunnel Communications channel 4) DSTC001 - GSL-STC-004								
79 Open network port expl	Unprotected network port(s) on network devices and connection points	Wireless Network device (Scop of HDO)	ie 1) Capture your account's user ID and credentials. 2) Log the data of online traffic accessed on your tablet or comput In this way, they can maintain a data of the websites you mostly v and plan attack from these websites.	uter. visit,																reless security	1. SOM D001020115 - 23. Malware Detection/Protection Penetration Testing Protoco Document #: D001020037: 2. SOM D001020115 - 11. 1) DSTC001: GSL-STC-001								
T10	V12	Aus	Gain access to your computer, its network and data. Launch a spam or malware attack on your device.		None	None Low	Network	High	Low	None	Unchanged	1.6	0.2	1.4	31	Moderate	0.5	23	options based on man	facture manual	Configuration settings 1) DSTC001: GSL-STC-032					#N/A	#N/A		
80 Open network port expl	Unencrypted Network segment through out the information flow	Tablet OS/network details & Tablet Application	Capture your account's user ID and credentials. Log the data of online traffic accessed on your tablet or compute In this way, they can maintain a data of the websites you mostly versions.	nA uter. visit,		\dashv													LOW 1. Asset should be beh firewall 2. Anti-virus with upd	ind stateful	1. SOM D001020115 - 23. Malware Detection/Protection Document #: D001020037:	d			+				
			and plan attack from these websites. 3) Gain access to your computer, its network and data. 4) Launch a spam or malware attack on your device.																definitions 3. Audit/System log ca	pturing any tified/reported by	2-SRS D001020024 - 2.17.6The Application shall support the use of anti-malware mechanism 2) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002								
Т10	V14	A02			None	None Low	Network	High	Low	None	Unchanged	1.6	0.2	1.4	31	Moderate	0.5	23	4. Use hardened inter	sications channel	3.SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware					#N/A	#N/A		
																					(SmartMedic devices). 3) DSTC001: GSL-STC-003 4. SRS D001020024 - 2.17.2The								
81 Open network port expl	oit Unencrypted data in transit in all flowchannels	Data in Transit	Capture your account's user ID and credentials.	NA NA															LOW 1. Use secure tunnel o	mmunication	Application shall provide secure tunnel Communications channel 4) DSTC001 - GSL-STC-004 1. SRS D001020024 - 2.17.2The Penetration Testing Protoco								
(TTP)	flowchannels		2) Log the data of online traffic accessed on your tablet or comput In this way, they can maintain a data of the websites you mostly v and plan attack from these websites. 3) Gain access to your computer, its network and data.	uter. visit,															channel 2. Configure and upgr. n/w security 3. Configure firewalls	de routers for the	Application shall provide secure tunnel Communications channel SRS D001020023 - 2.13.3The Application shall provide secure 1) DSTC001: GSL-STC-004								
																			packets with spoofed 4. Maintain access cor permission list for any unencrypted data if pr	iddresses. trol (read/modify) sensitive & esent.	tunnel Communications channel 2) DSTC001: GSL-STC-004 2. SOM D001020115 - 16. Transmission confidentiality and								
T10	V17	A10			None	None Low	Network	High	Low	None	Unchanged	1.6	0.2	1.4	31	Moderate	ū.s	23	5. For sensitive data p mechanism needs to b designed & implemen	oper encryption	Integrity 4) DSTC001: GSL-STC-001 3. SOM D001020115 - 23. Malware 5) DSTC001: GSL-STC-017 Detection / Protection					#N/A	#N/A		
																					Detection/Protection 4. SOM D001020115 - 05. Access control policy and management 6) DSTC001: GSL-STC-006								
82 Open network port expl	oit Insecure communications in	Tablet OS/network details &	Capture your account's user ID and credentials.	NA NA							1								LOW 1. Asset should be beh	ind stateful	S.SAD/SDD-D001020099-6.7 Security* 1.SOM D001020115 - 23. Malware Penetration Testing Protoco	d							
(TTP)	networks (hospital)	Tablet Application	2) Log the data of online traffic accessed on your tablet or computed in this way, they can maintain a data of the websites you mostly vand plan attack from these websites. 3) Gain access to your computer, its network and data.	uter. visit,															firewall 2. Anti-virus with upd definitions 3. Audit/System log co	ited virus	Detection/Protection Document #: D001020037: 2-SRS D001020024-2-17.6The Application shall support the use of								
Т10	vos	A02	Launch a spam or malware attack on your device.		None	Low Low	Network	High	Low	None	Unchanged	1.6	0.4	25	42	Moderate	0.5	3.4	abnormal activity idea the application 4. Use hardened inter	tified/reported by laces (n/w) & sications channel	anti-malware mechanism 2) DSTC001: GSL-STC-002 3.SRS D001020024 -2.22.1 The Apolication shall have loss of tablet					#N/A	#N/A		
																			and the same		Application small naive logs of camera application and firmware (SmartMedic devices). 4. SRS D001020024-2.17.2The								
																					4. SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel								

Stopher Grandsmit

	-		Adverse Impact		the little	. 8						Pre-Implementation of Secu	urity Controls							S	ecurity Controls/Mitigations		lity	2		Post-Impl	ementation of Security Contro	is		
ID # Threat Event(s) 83 Brute-force Attack	Vulnerabilities Devices with default passwords	Asset Smart medic app (Stryker Adm	Impact Description in 1] An attacker may attempt to discover a weak credential by	Safety Impact (Risk ID# or N/A)	Confidentia	Integrity Availabili	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Low 1. During	the access providing, if default	Implementation of Risk Control Measures 1. Have to be closed before DR-8	Measures (Effectiveness) Penetration Testing Protocol	Confidentia	Attack 1	ector Attack Pr Complexity Re	ivileges User quired Interaction	Scope CVSS v3 Sco	i.0 Base Overa	ll Risk Security Risk re Level	Residual Security Risk Acceptability Justification
(CAPEC-112)	needs to be checked for brusteforce attacks	Web Application)	systematically trying every possible combination of letters, numb- and symbols until it discovers the one correct combination that works.	ers,	Low	None Low	Network	High	High	None	Unchanged	67	0.4	25	13	Moderate	as	29	changing t Also ensur 2. Require 3. Limit au Limiting) 4. Audit, 5/5 logs (login change) 5. Audit, 5/5 logs (such	are: e multi-factor authentication suthentication attempts (rate) System log - Maintain Access in (attempted & failed), logoff, id System log - Maintain security has change/modification of onfiguration settings, services,	2. SRS D001020097 - 2.1.2.6 The Application shall be validated by using an invisible captcha during	2) DSTC001: GSL-STC-025 iid 3) DSTC001: GSL-STC-009 4) DSTC001: GSL-STC-014 5) DSTC001: GSL-STC-031 6) DSTC001: GSL-STC-031					eN	1/A #N	/A	
84 Brute-force Attack (CAPEC-112)	Devices with default passwords needs to be checked for bruteforce attacks	Smart medic app (Azure Portal Administrator)	An attacker may attempt to discover a weak credential by systematically tyring every possible combination of letters, manh and ymbols until it discovers the one correct combination that works.	NA NA	Low	None Low	Network	High	High	None	Unchanged	0.7	0.4	25	33	Moderate	85	29	password changing t Also ensum 2. Require 3. Limit au Limiting) 4. Audit/S logs (logic change) 5. Audit/S logs (segin	d is provided then immediately the password is needed. are: re multi-factor authentication authentication attempts (rate	The setup & configuration process of azure cloud & admin shall be documented and published within to organization for the corresponding teams using the admin portal	Document #: D001020037: he					sh	1/A #N	i/A	
85 Brote-force Attack (CAPEC-112)	The pastword complexity or location vulnerability. Like weak pastwords and hardcoded pastwords.	Smart medic app (Stryker Adm Web Application)	in 1) An attacker may attempt to discover a weak credential by systematically tyring every possible combination of letters, numbard symbols until it discovers the one correct combination that works.	NA NA	Low	None Low	Network	Nigh	High	None	Unchanged	0.7	0.4	25	13	Moderate	as	29	recommer 2. Require 3. Limit au Limiting) 4. Audit, ½ logs (logir change) 5. Audit, ½ logs (such system cor etc.)	ended for admin web app. - multi-factor authentication suthentication attempts (rate) System log - Maintain Access in (attempted & failed), logoff, id System log - Maintain security h as charged/modification of onliguration settings, services, yer authentication methods	1. Have to be closed before DR-8 2. SSIS D001020997 - 2.1.2.6 The Application shall be validated by the company of the company of the company of the company 3. SISS D001020997 - 2.1.2.1.1 Impals canall or password, only 3 attempts 64. SISS D001020997 - 2.2.2.2 Audit logs 5. SISS D001020997 - 2.2.2.2 Audit logs 6. SLD/SDD-D001020999-6.7	2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-031 5) DSTC001: GSL-STC-031					45	I/A =N	//A	
86 Brute-force Attack (CAPEC-112)	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Smart medic app (Azure Portal Administrator)	1) An attacker may attempt to discover a weak credential by systematically typing every possible combination of letters, numband symbols until it discovers the one correct combination that works.	NA NA	Low	None Low	Network	High	High	None	Unchanged	87	0.4	25	33	Moderate	ės	29	3. limit au Limiting) 4. Audit; 75 logs (logic change) 5. Audit; 75 logs (such system cor etc.)	password strength practices is ended in azure e multi-factor authentication uthentication attempts (rate	Security* The setup & configuration process of azure cloud & admin shall be a configuration or control and a configuration of the configuration for the corresponding teams using the admin portal	of Penetration Testing Protocol Document 6: D001020037: lat 1) DSTC000: GSL-STC-029					eh.	I/A sh	i/A	
87 Broins force Attack (CAPEC-112)	Week Discryption Implementation in the control of t	Data at Rest	An attacker may attempt to discover a weak encryption by systematically trying every possible combination of discryption be described to the description of the description of the description in the	ry. NA	Low	None Low	Local	High	High	None	Unchanged	05	84	25	30	Moderate	65	28	for azure) 2. Proper 3. Encrypt for ex: wh storage, et 4. Transfe	Congress of entroped access countries of the congress of the c	1. IKSA. SDD-000120110-4.22-Anni Clored Infrastructure Clored Infrastructure Control policy and management State (1997) and management Tables SDD-000120000-6.7 Security Tables SDD-0001200011-4.7 Security Tables SDD-0001200011-4.7 Security ASS DD-0001200011-4.7 Security SDD-0001200011-4.7 Security SDD-0001200011-4.7 Security SDD-0001200011-4.7 Security SDD-0001200110-4.2 Substitute Control SDD-0001200110-4.2 Substitute Control SDD-0001200011-6.7 Security	1) BST0091: GSL STC-020 2) BST0091: GSL STC-017 3) BST0091: GSL STC-066 4) BST0091: GSL STC-066 6) BST0091: GSL STC-064 6) DSTC091: GSL STC-064 7) BST0091: GSL STC-064 9) BST0091: GSL STC-094 9) BST0091: GSL STC-094						/A sn	//A	
88 Brute-force Attack (CAPEC-132)	Weak Encryption Implementation in data at creat and in trainit factors and in trainit factors and of design wines. V28	Data in Yransik	An attacker may attempt to discover a weak encryption by systematically trying every possible combination of decryption he	ey. NA	Low	None Low	Network	High	High	None	Unchanged	0.7	0.6	25	33	Moderate	85	29	Configu n/w secur Configu packets w	ure and upgrade routers for the ority ure firewalls to reject any with spoofed addresses. cure tunnel communication	2. SOM D001020115 - 16. Transmission confidentiality and	Penetration Testing Protocol Document 8: 1001/20037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-016 3) DSTC001: GSL-STC-001 4) DSTC001: GSL-STC-004					øx.	1/A #N	//A	
89 Social Engineering (TTP) T12	Legacy system identification if any	Smart medic app (Stryker Adm Web Application)	in 1) This threat may hamper digital or physical resources, infractivative and end points 2) Get the user (employee) client/ customer) to download malwa send money or perform actions that are dangerous.	NA sre,	None	Low High	Adjacent Network	High	High	Required	Unchanged	0.4	0.7	42	46	Moderate	ūS	45	2. Stateful 3. Disable 4. Maintai permissio	ill firewall e device network discoverable sin access control (read/modify)	Using web app the admin can able to view the functionality of different components existing in the SM platform. Admin app doesnt control any of the system components, the control any of the system components when the risk associated to the SM platfor with admin web app can be ignored.	1) DSTC001: GSL-STC-029					aN	1/A #N	//A	
90 Social Engineering (TTP) T12 91 Lack of evidence to conclude	Checking authentication modes for possible hacks and bypasses V04	A07	3) The threat may hamper digital or physical resources infection trans and opinist through perspitating mail infection trans and opinist through perspitating mail 2 (left the sure (employee) client (extension) to download malware seed moneyor perform actions that are dangerous. 3) Reputational harm 4) Economical harm 11. Adversary tried to obtain knowledge about events instruction.		None	Low High	Adjacent Network	High	High	Required	Unchanged	0.4	0.7	42	46	Moderate	ů5	45	1. Set your high 2. Restrict to unauth 3. Restrict 3rd party: mails, etc. 4. Configu	ur spam filters setting options to to the system getting connected henticated sources to the system in accessing the yites, social engineering sites, c. ure firewalls to reject any with snoofed addresses.	The setup & configuration process of azure cloud admins shall be documented and published within the organization for the corresponding teams using the admin portal The setup & configuration process of	Document #: D001020037: hee 1) DSTC001: GSL-STC-029					σN	1/A #N	I/A	
91 Lack of evidence to conclude any multi-close steemy/statick (ST(R,HDE)	Insufficient Logging Information	Smart menic app (Azure Portal Administrator)	Adversary free to octate sourceage about system internase Statement to find attack vectors Statement to find attack vector find attacker/mallicious activities in recorded recorded to find attacker/mallicious activities in recorded		Low	Low Low	Lecal	Low	Low	None	Unchanged	18	0.5	34	ន	Low	02	38	All the infi identifying and adver- logged for and attack the system	formation needed for	The setup & consiguration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Document #: D001020037:					ah	1/A #N	I/A	
92 Lack of evidence to conclude any malicious attempt/attack (ST(R]IDE)	Insufficient Access permissions for accessing and modifying Log files	Smart medic app (Azure Portal Administrator)	Abstractly the direct obtain knowledge about system internals: Abstractly for the fatch excurse: Standard for the fatch excurse: Standard for fatch excursed an abstract for the standard fatch of the standard fatch for the standard fatch fatch for the standard fatch fatch for the standard fatch	NA NA	Low	Low Low	Local	Low	Low	None	Unchanged	18	0.5	34	53	Low	02	38	All the is identifying and advers logged for and attack the system correcting Audit/S	information needed for ng the threat (malicious) activity	organization for the corresponding	Document #: D001020037: he					sx	1/A #N	1/A	
93 Gaining Access ([S]TRID[E])	Error Info containing sensitive data for Failed Authentication attempts V24	Smart medic app (Azure Portal Administrator)	An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbrols and and symbols until it discovers the one correct combination that works.	NA NA	Low	Low High	Network	High	Low	None	Unchanged	16	0.7	47	6.4	Moderate	0.5	5.6	be used. In should be	Information aiding the attacks e avoided. from user id there should be al security factor for verification. on the login attempts is	documented and published within th	Document #: D001020037: he					πN	1/A #N	I/A	
94 Gaining Access ([S]TRID[E]) T03	Improper security (for ex.,Storage & Access) for Key tokens and Certificates V30	Azure Cloud DataBase	I) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numb and symbols until it discovers the one correct combination that works.	NA NA	Low	Low High	Network	High	Low	None	Unchanged	16	0.7	47	6.4	Moderate	0.5	5.6	MEDIUM 1. If databases/certistorage sh 2. Apart fr	base access using	1.2. SAD - D001020031 - 2.2.1.7 - Cosmos DB 3. Have to be closed before DR-8	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-027 2) DSTC001: GSL-STC-029					πN	I/A #N	I/A	
95 Gaining Access ((Syrton (e)) T03	Absence of additional security factor along with user identification V25	Smart medic app (Azure Portal Administrator)	I) he anseler may attempt to discover a weak crediential by spanning the discovers possible conductation of terrors, cando and symbols until it discovers the one correct combination that works.	NA NA	Low	Low High	Network	High	Low	None	Unchanged	16	0.7	er	64	Moderate	0.5	5.6	mandator I. Azure p credential password required 2. If datable keys/cert storage sh 3. Apart fr additional	CC. portal can be accessed by login als & MFA. Hence, strong d policies & management are base access using tificates, their generation & hould be done securely. The desired is accessed as access to the securely force user if there should be alsecurity factor for verification, on the login attempts is	The setup & configuration process or azure cloud & admin shall be documented and published within it organization for the corresponding teams using the admin portal	of Penetration Testing Protocol					sh	/A #N	//Д	

Stepher Cantalonnial

				Adverse Impact									Pre-Implementation of Securi	to Control								Security Controls/Mitigations						Post Innionantal	of Security Controls			
ID#	Threat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Integrity	Attaci	k Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score		Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures		Verification of Risk Control Measures (Effectiveness)	Onfidentiality	Attack Vecto	r Attack Complexity	Privileges Required	User	ope CVSS v3.01 Score	Base Overall	Risk Security Risk Level	Residual Security Risk Acceptability Justification
96	Gaining Access ([S]TRID[E])	Absence of additional security factor along with user identification	Azure Cloud DataBase	1) An attacker may attempt to discover a weak credential by systematically tyring every possible combination of letters, numbin and symbols until it discovers the one correct combination that works.	NA Low	Low	High Net	bwork	High	Low	None	Unchanged	16	0.7	47	64	Moderate	0.5	5.6	MEDIUM	If database access provided & also using keys/certificates, their generation & storage should be done securely. Apart from user id there should be additional security factor (keys/certificates) for verification. I Limit on the login attempts is mandatory.		Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-027 2) DSTC001: GSL-STC-027 3) DSTC001: GSL-STC-029						#N/A	. #N/:	A	
97	Brute-force Attack (CAPEC-112)	Error Info containing sensitive data for Failed Authentication attempts	Azure Cloud DataBase	1) An attacker may attempt to discover a weak credential by optimizing typing every possible combination of letters, numbian and symbols until it discovers the one correct combination that works.	NA Low		High Net	twork	High	Low	None	Unchanged	16	0.7	4.7	6.4	Moderate	0.5	5.6	MEDIUM	Standard error info messages should be used information aiding the attacks should be avoided. Apart from user id there should be additional security factor for verification. It limit on the login attempts to mandatory.	messages should be displayed upon validation of credentials to mitigate the risk of account harvesting and	Document #: D001020037:						#N/A	. #N/s	A	
98	Brute-force Attack (CAPEC-112)	Having no limit on the login attempts	Smart medic app (Azure Portal Administrator)	1.) As attacker may attempt to discover a weak credential by systematically prigore every possible confusions of letters, maintained on letters, maintained on letters, maintained and symbols until it discovers the one correct combination that works.	Low		High Net	twork	High	Low	None	Unchanged	16	0.7	4.7	6.4	Moderate	0.5	5.6	MEDIUM	Standard error info messages should be used. Information aiding the attacks should be avoided. Apart from user id there should be additional security factor for verification. Limit on the login attempts is mandatory.	of azure cloud & admin shall be documented and published within th organization for the corresponding	Document #: D001020037: e 1) DSTC001: GSL-STC-018 2) DSTC001: GSL-STC-027 3) DSTC001: GSL-STC-029						#N/A	. #N/s	A	
99	Unauthorized Alterations (S[T]RIDE)	Improper/incufficient provisioning of IOT hub	Tablet OS/network details & Tablet Application A02	I. If provisioning get falled/miseleded then the complete functionality get affected. Proper reason for the provisioning failure needs to addressed.	NA None		High Net	bwork	High	High	None	Unchanged	0.7	0.6	3.6	44	Low	0.2	38	LOW	A. All devices which need to be registered by the control of the process of the provisioning one of the process of the provisioning of the process of t		Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-026						#N/A	. #N//	Α	
100	Unauthorized Alterations (S[T]RIDE)	Unsecured communication with unauthenticated 3rd party devices		When is no proper authentication between the devices in the or mande enrollment to the dayrup devices can easily establish the communication with the stryker devices.	art NA	None		twork	High	High	None	Unchanged	0.7	0.6	3.6	44	Low	0.2	38	LOW	In complete must made de environment only authenticated stryker and Blood devices need to be present Secure communication between the stryker devices needs to be established didocumented 3. Bandling of the unauthenticated and pury devices trying to communicate with any part devices needs to be taken care of the party devices trying to communicate with any part devices needs to be taken care.	SRS D001020024 - 2.17.8 - Only Stryker made/ authenticated devices should be able to communicate with SM device and tablet. SRS D001020024 - 2.17.8 - Only	Document #: D001020037: 1) DSTC001: GSL-STC-030 2) DSTC001: GSL-STC-010 3) DSTC001: GSL-STC-010						sn/A	. #N/.	A	

Styler Continuits Page 1

Security Risk Assessment Summary

ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
5	T01	Deliver undirected malware (CAPEC-185)	V22	Legacy system identification if any	A03	Smart medic (Stryker device) System Component	Malicious utilization of computer resources 2) computing power denial of service attacks, ransomware attack Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
6	T01	Deliver undirected malware (CAPEC-185)	V22	Legacy system identification if any	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
7	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
8	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
9	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A03		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
10	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		

Stryker Confidential Page 14 of 27

ID#		Threat Event(s)		Vulnerabilities	Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
11	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
12	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
13	T01	Deliver undirected malware (CAPEC-185)		Unprotected network port(s) on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
14	T01	Deliver undirected malware (CAPEC-185)		Unprotected network port(s) on network devices and connection points	Smart medic (Stryker device) System Component	Malicious utilization of computer resources 2) computing power denial of service attacks, ransomware attack Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
15	T01	Deliver undirected malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	Application, Network interfaces	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
16	T01	Deliver undirected malware (CAPEC-185)	V17	Unencrypted data in transit in all flowchannels	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
17	T01	Deliver undirected malware (CAPEC-185)	V17	Unencrypted data in transit in all flowchannels	Application, Network interfaces	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		

Stryker Confidential Page 15 of 27

ID#	Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
18	T01 Deliver undirected malware (CAPEC-185)	V23	Outdated - Software/Hardware	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		·
19	T01 Deliver undirected malware (CAPEC-185)	V23	Outdated - Software/Hardware	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
20	T01 Deliver undirected malware (CAPEC-185)	V23	Outdated - Software/Hardware	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
21	T02 Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		Justification
22	T02 Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
23	T02 Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
24	T02 Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A08	Wireless Network device (Scope of HDO)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	SOM responsibility 1. Statefull Firewall 2. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present.		

Stryker Confidential Page 16 of 27

ID#	Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
	T02 Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		juotineuton
26	T02 Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A11	Smart medic app (Stryker Admin Web Application)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
27	T02 Deliver directed malware (CAPEC-185)	V02	External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	MEDIUM	Only stryker made/authenticated devices should communicate with smart medic device & tablet Asset should be behind stateful firewall Use secure tunnel communications channel		
28	T02 Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
29	T02 Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
30	T02 Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Application, Network interfaces	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
31	T02 Deliver directed malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	MEDIUM	Only Stryker/HDO authenticated devices should communicate with smart medic device & tablet Asset should be behind stateful firewall Use secure tunnel communications channel		

Stryker Confidential Page 17 of 27

ID#	Threat Event(s)	Vulr	nerabilities	Assets	Impact Description		Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
32	T02 Deliver directed malware (CAPEC-185)		ted network n network nd connection	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA		LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		,
33	T02 Deliver directed malware (CAPEC-185)		are/OS on evices, Laptops,		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA		LOW	1. Deployed (V&V) secure system configuration model needs to be mentioned in the installation manual. 2. Establish internal and external information sources for threat intelligence and vulnerability data, monitoring them regularly and taking appropriate action for high-priority items 3. Use upgraded software, firmware 4. Never create/use credentials with personal details such as date of birth, spouse, or child's or pet's name 5. Stateful Firewall		
34	T02 Deliver directed malware (CAPEC-185)		are/OS on evices, Laptops,	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA		LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
35	T02 Deliver directed malware (CAPEC-185)		oted data at rest sible locations	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA		LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
36	T02 Deliver directed malware (CAPEC-185)		oted data at rest sible locations		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA		LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
37	T02 Deliver directed malware (CAPEC-185)		oted data at rest sible locations		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA		LOW	Identification of the sensitive data in storage and encryption of storage subsystem Stateful firewall Hardening of the host system containing sensitive data at rest Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. Use strong encryption algorithm		

Stryker Confidential Page 18 of 27

ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description		Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
38	Т03	Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	(11011121111111111111111111111111111111	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		juounouton
39	Т03	Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A11	Web Application)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA		MEDIUM	1. Admin application can be accessed by login credentials & MFA. Hence, strong password policies & management are required 2. Data transfer between the admin application and the smart medic components needs to be encrypted & secured. 3. Any vulnerable network ports and connection points should be identified and hardened. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Stateful firewall		
40	Т03	Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA		LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
41	Т03	Gaining Access ([S]TRID[E])	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA		MEDIUM	1.During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Maintain Access Logs		
42	Т03	Gaining Access ([S]TRID[E])	V01	Devices with default passwords needs to be checked for bruteforce attacks	A07	Interface/API Communication	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA		LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		

Stryker Confidential Page 19 of 27

ID#	Threat Event(s)		Vulnerabilities	Assets	Impact Description		Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
	T03 Gaining Access ([S]TRID[E])	I I	complexity or location vulnerability. Like weak passwords and hardcoded passwords.		Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA		MEDIUM	1. If devices/apps being accessed by login credentials & MFA. Then, strong password policies & management are required 2. Require multi-factor authentication 3 Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		
44	T03 Gaining Access ([S]TRID[E])	1	Checking authentication modes for possible hacks and bypasses	Authentication/Authorisation method of all device(s)/app	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA		LOW	1. Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks 2. Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks 3. Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks 4. Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration		
45	T03 Gaining Access ([S]TRID[E])	1	Checking authentication modes for possible hacks and bypasses	Web Application)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA		LOW	Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration		
46	T03 Gaining Access ([S]TRID[E])	1	Checking authentication modes for possible hacks and bypasses	Smart medic app (Azure Portal Administrator)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA			Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration		

Stryker Confidential Page 20 of 27

ID#	Threat Event(s)	Vulnerabilities	Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
	T03 Gaining Access ([S]TRID[E])	V13 Unprotected external USB Port on the tablet/devices.	A01 Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		,
48	T04 Maintaining Access (TTP)	V01 Devices with default passwords needs to be checked for bruteforce attacks	Authentication/Authorisation method of all device(s)/app	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		
49	T04 Maintaining Access (TTP)	V03 The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A04 Authentication/Authorisation method of all device(s)/app	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	1. If devices/apps being accessed by login credentials & MFA. Then, strong password policies & management are required 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		
50	T05 Clearing Track (TTP)	V21 InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01 Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	NA F	LOW	Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
51	T05 Clearing Track (TTP)	V23 Outdated - Software/Hardware	A01 Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
52	T05 Clearing Track (TTP)	V07 Lack of configuration controls for IT assets in the informaion system plan	A01 Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		

Stryker Confidential Page 21 of 27

ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
		Clearing Track (TTP)	V07	Lack of configuration controls for IT assets in the informaion system plan	A05	Device Maintainence tool (Hardware/Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
54		Clearing Track (TTP)		Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
55		Clearing Track (TTP)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware/Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
56		Clearing Track (TTP)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A02	Tablet OS/network details & Tablet Application	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
57	T05	Clearing Track (TTP)		The static connection digaram between devices and applications with provision for periodic updation as per changes	A05	Device Maintainence tool (Hardware/Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
58		Clearing Track (TTP)		The static connection digaram between devices and applications with provision for periodic updation as per changes	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
59		Elevation of privilege (STRID[E])	V15	Controlled Use of Administrative Privileges over the network		Authentication/Authorisation method of all device(s)/app	1) Gaining access to the portal 2) Accessing confidential data, 3) Lead misuse of confidential data 4) Company defamation	NA	LOW	Require that administrators establish multi factor authentication for their administrator and non-administrative accounts. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. Ensure default credentials not existing for any assets (such as applications, operating systems, routers, firewalls, wireless access points).		

Stryker Confidential Page 22 of 27

ID#	Threat Event(s)		Vulnerabilities		Assets	Impact Description		Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
	T06 Elevation of privilege (STRID[E])	V15	Controlled Use of Administrative Privileges over the network	A12	Smart medic app (Azure Portal Administrator)	1) Gaining access to the portal 2) Accessing confidential data, 3) Lead misuse of confidential data 4) Company defamation	NA		MEDIUM	Require that administrators establish multi factor authentication for their administrator and non-administrative accounts. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. Ensure default credentials not existing for any assets (such as applications, operating systems, routers, firewalls, wireless access points).		juomituutoi.
61	T07 Denial of service (STRI(D)E)	V12	Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	Bring down the service availability Blocking the end user usage	NA		MEDIUM	Asset should be behind stateful firewall Anti-virus with updated virus definitions System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
62	T08 Information disclosure (STR(I)DE)	V16	Unencrypted data at rest in all possible locations	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc	NA		LOW	Identification of the sensitive data in storage and encryption of storage subsystem Stateful firewall Hardening of the host system containing sensitive data at rest Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. Use strong encrption algorithm		
63	T08 Information disclosure (STR(I)DE)	V17	Unencrypted data in transit in all flowchannels	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	NA		LOW	1. Use secure tunnel communication channel 2. Configure and upgrade routers for the n/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. For sensitive data proper encryption mechanism needs to be designed & implemented		
64	T08 Information disclosure (STR(I)DE)	V18	Weak Encryption Implementaion in data at rest and in transit tactical and design wise	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc	NA		LOW	1. Implement server-side encryption using Service-Managed keys/recomended practise by azure. 2. Proper way of network access control 3. Encryption for sensitive data in transit, for ex: when files are moved to cloud storage, etc 4. Transfer over encrypted tunnel 5. Use strong encryption algorithm		
65	T08 Information disclosure (STR(I)DE)	V18	Weak Encryption Implementaion in data at rest and in transit tactical and design wise	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	NA		LOW	Statefull firewall Configure and upgrade routers for the n/w security Configure firewalls to reject any packets with spoofed addresses. Use secure tunnel communication channel		

Stryker Confidential Page 23 of 27

ID#	Threat Event(s)	Vulnerabilities	Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability [Ustification]
	T08 Information disclosure (STR(I)DE)	V19 Weak Algorthim implementation with respect cipher key size	A09 Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	1. Weak algorithms such as DES, RC4, etc should be avoided and usage of strong algorithms such as AES, RSA, etc are recomended 2. Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.	10012070	juounouton
67	T08 Information disclosure (STR(I)DE)	V19 Weak Algorthim implementation with respect cipher key size	A10 Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	1. Weak algorithms such as DES, RC4, etc should be avoided and usage of strong algorithms such as AES, RSA, etc are recomended 2. Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.		
68	T08 Information disclosure (STR(I)DE)	V21 InSecure Configuration for Software/OS on Mobile Devices, Laptops Workstations, and Servers	A01 Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
69	T08 Information disclosure (STR(I)DE)	V14 Unencrypted Network segment through out th information flow	A10 Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	1. Anonymization/Pseudomyzation of patient details 2. Data encyrption 3. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 4. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.)		
70	T08 Information disclosure (STR(I)DE)	V05 Insecure communications in networks (hospital)	A10 Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	Secure communication with Secure Sockets Layer (SSL) or TLS protocols that provide message confidentiality Secure sensitive data in the channel flow using strong encryption Statefull firewall Proper way of network access control		
71	T09 Data Access (STR[I]DE)	V12 Unprotected network port(s) on network devices and connection points	A01 Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Allowing application or script to perform abnormal activites on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		
72	T09 Data Access (STR[I]DE)	V12 Unprotected network port(s) on network devices and connection points	A02 Tablet OS/network details & Tablet Application	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		

Stryker Confidential Page 24 of 27

ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
73	T09	Data Access (STR[I]DE)		Devices with default passwords needs to be checked for bruteforce attacks	A09		Allowing application or script to perform abnormal activites on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.		LOW	During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: Statefull firewall Do not store sensitive data in plaintext. Use strong encrption algorithm. Apply salting over sensitive data.		
74	Т09	Data Access (STR[I]DE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	method of all device(s)/app	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	MEDIUM	During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: Statefull firewall Do not store sensitive data in plaintext. Use strong encrption algorithm. Apply salting over sensitive data.		
75	Т09	Data Access (STR[I]DE)		Devices with default passwords needs to be checked for bruteforce attacks	A10		1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	LOW	During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: Statefull firewall Do not store sensitive data in plaintext. Use strong encrption algorithm. Apply salting over sensitive data.		
76	Т09	Data Access (STR[I]DE)		The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A09		1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	LOW	Strong password strength practices is recommended for admin web app. Require multi-factor authentication Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Stryker Confidential Page 25 of 27

Common Vulnerability Scoring System (CVSS v3.0)

	Exploitability Metrics											
Attack '	Vector		Attack Complexity			Privelege Required				User Interaction		
Metric Value Code		Metric	Value	Code	Metric	Value		Code	Metric	Value	Code	
Network	0.85	N	Low	0.77	L	None	0.85	0.85	N	None	0.85	N
Adjacent Network	0.62	A	High	0.44	Н	Low	0.62	0.68	L	Required	0.62	R
Local	0.55	L				High	0.27	0.5	Н			
Physical	0.2	P										

	Technical Impact Metrics							
Confidentiality	Confidentiality, Integrity, Availability Impact							
Metric	Value	Code						
None	0	N	$ISC_{Base} = 1 - [(1-Impact_{Conf}) \times (1-Impact_{Integ}) \times (1-Impact_{Avail})]$					
Low	0.22	L						
High	0.56	Н						

Scope								
Unchanged	An exploited vulnerability can only affect resources managed by the same authority. In this case the vulnerable component and the impacted component are the same.	U						
Changed	An exploited vulnerability can affect resources beyond the authorization privileges intended by the vulnerable component. In this case the vulnerable component and the impacted component are different.	С						
		✝						

ASSUMPTIONS:

Base metrics

For the purposes of the medical device only Base metrics are considered. The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics. The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.

The document only considers the mandatory base metric since the device is typically utilized in tightly controlled user environments such as hospitals and this is already a consideration of this assessment document. The changing charecteristics of vulnerabilities will be assessed seperately through the software development lifecycle

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Likelihood of Attack Initiation								
	Rating	Score						
	Very Low	0.04						
	Low	0.20						
	Moderate	0.50						
	High	0.80						
	Very High	1.00						

In Scope	Yes	Ī
	No	

Stryker Confidential Page 26 of 27

Threat Sources

	Adversarial Threat		Non-Adverserial Threat					
ID#	Threat Source	In Scope (Y/N)	ID#	Source	In Scope (Y/N)			
TSA-1	Individual (Disgruntled/Ex-Employees, Outsider, Insider, Trusted Insider, Priveleged Insider)	Y	TSN-1	Accidental (Priveleged User/Administrator, inexperienced user, inexperienced installer, inexperienced maintainer, unintentional misuse)	Y			
TSA-2	Organization (Competitor, Supplier, Partner, Customer, Researcher)	Y	TSN-2	Researchers (Professional Security, Academic)	Y			
TSA-3	Script Kiddies	Y	TSN-3	Vulnerable systems/devices connected to device (e.g., via RS-232, USB, or other connections)	Y			
TSA-4	Political Activists (Hactivists, Anonymous, Wikileaks)	N	TSN-4	Incompatible Software (OS, Networking, Applications)	Y			
TSA-5	Organized Crime (Cyber Terrorists)	N	TSN-5	Environmental Impact (IT equipment, Temperature/Humidity Controls, RF Interference)	Y			
TSA-6	Nation States	N	TSN-6	Natural/Man-Made Disaster (Fire, Flood/Tsunami, Windstorm/Tornado, Earthquake, Bombing, Telecommunications/Power Failure)	N			

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Stryker Confidential Page 27 of 27